GFI MailEssentials 14.1

Administrator- und Konfigurationshandbuch

GFI Software Ltd.



http://www.gfi.com
E-Mail: info@gfi.com

Version ME-ACM-DE-1-02.003

Letzte Aktualisierung: 19. Oktober 2009

Inhalt

1 Informationen zu GFI MailEssentials

1.1 Einführung

GFI MailEssentials ist eine Server-Anti-Spam-Lösung, die Ihren Mailserver durch wichtige Anti-Spam-Funktionen für Firmen-E-Mail ergänzt. Als Zusatz zu Ihrem Mailserver ist GFI MailEssentials komplett benutzertransparent, eine zusätzliche Schulung der Benutzer ist nicht erforderlich.

Haupteigenschaften dieser Lösung:

- **Servergestützte Anti-Spam-Lösung** - Spamschutz ist ein wichtiger Teil der Sicherheitsstrategie für Ihr Netzwerk. GFI MailEssentials bietet moderne Spam-Filter, beispielsweise mit Blacklist und Whitelist, Bayes-Filter, Keyword-Prüfung und Header-Analyse.
- **Unternehmensweit einheitlicher Haftungsausschluss und Fußzeilentext -** Unternehmen haften für den Inhalt der E-Mail-Mitteilungen ihrer Mitarbeiter. Mit GFI MailEssentials können Haftungsausschlüsse automatisch am Anfang oder Ende einer E-Mail eingefügt werden, ebenso Felder und Variablen, die den Haftungsausschluss für den Empfänger entsprechend anpassen.
- **E-Mail-Archivierung in Datenbank** - Die Archivierung von E-Mails hat sich nicht nur in der Praxis bewährt, sondern ist ggf. auch gesetzlich vorgeschrieben. GFI MailEssentials bietet die Möglichkeit, alle eingehenden und ausgehenden E-Mails zu archivieren.
- **Berichterstellung -** GFI MailEssentials kann verschiedene nützliche Berichte zur Nutzung von E-Mail und zur Spam-Bekämpfung erzeugen.
- **Personalisierte automatische Antworten mit Referenznummer** - Automatische Antworten können nicht nur mitteilen, dass gerade niemand im Büro ist, sondern den Kunden informieren, dass seine E-Mail eingegangen ist und die Anfrage beantwortet wird. Ordnen Sie jeder Antwort eine eindeutige Referenznummer zu, damit Kunden und Mitarbeiter Nachrichten einfacher finden.
- **POP3-Downloader -** Kleinunternehmen haben möglicherweise nicht die entsprechenden Systeme zur Nutzung von SMTP-E-Mail. GFI MailEssentials enthält ein Modul, das E-Mails von POP3-Postfächern abrufen und in Postfächer auf dem Mailserver verteilen kann.
- **E-Mail-Überwachung** - Zentrale Datenspeicher lassen sich in der Regel einfacher verwalten als verteilte Informationen. GFI MailEssentials erlaubt für die E-Mail-Nachrichten einer bestimmten Person oder Abteilung den Versand von E-Mail-Kopien an einen zentralen Speicher.

Weitere Informationen zur Filterfunktion von GFI MailEssentials für eingehende und ausgehende E-Mails finden Sie in Anhang 1 - Wie funktionieren Spam-Filter? in diesem Handbuch

1.2 Verwendung dieses Handbuchs

Dieses Benutzerhandbuch ist eine ausführliche Anleitung, die die Systemadministratoren bei Konfiguration und Nutzung von GFI MailEssentials möglichst umfassend unterstützen soll. Dieses Handbuch baut auf den Hinweisen auf, die Sie in der 'Kurzanleitung für GFI MailEssentials' finden und beschreibt die Konfigurationseinstellungen, die Systemadministratoren vornehmen müssen um die Software optimal zu nutzen.

Dieses Handbuch enthält folgende Kapitel:

Kapitel 1	Vorstellung dieses Handbuchs
Kapitel 2	Es enthält detaillierte Informationen zu den Routine-Administrationsaufgaben, die Administratoren täglich ausführen müssen.
Kapitel 3	Es enthält detaillierte Informationen, wie GFI MailEssentials kundenspezifisch angepasst wird. Dazu gehört die Anpassung der Spam-Filter und der betreffenden Aktionen sowie der Haftungsausschlüsse und der automatischen Antworten.
Kapitel 4	Es enthält detaillierte Informationen, wie weitere Wartungsarbeiten und Konfigurationsaufgaben durchzuführen sind, die in den beiden ersten Kapiteln nicht erläutert wurden. Dazu gehört beispielsweise die Konfiguration der Funktion P2E, der E-Mail-Überwachung und der Remote-Befehle.
Kapitel 5	Dieses Kapitel enthält Hinweise zur Problembehandlung und zur Anforderung von Support sowie zur Beseitigung häufiger Probleme.
Anhänge	Die Anhänge enthalten weitere Informationen zur Funktion von Spam-Filtern und Bayes-Filtern sowie Informationen zu MSMQ.

1.3 Registrierung

Informationen zur Registrierung erhalten Sie hier:

http://www.gfi.com/products/gfi-mailessentials/pricing/licensing

1.4 Mindestanforderungen und Installation

Informationen zu Systemanforderungen und zur Installation finden Sie in der 'Kurzanleitung für GFI MailEssentials'.

2 Empfohlene Maßnahmen nach der Installation

2.1 Einführung

Informationen über Spam-Filter

GFI MailEssentials enthält standardmäßig bereits eine Reihe spezieller Spam-Filter. Jeder einzelne dieser Filter ist für eine bestimmte Art von Spam-Mails gedacht. Zusammen mit GFI MailEssentials werden folgende Filter ausgeliefert:

Filter	Beschreibung	Standard-mäßig aktiviert
SpamRazer	Ein Spam-Filter, der erkennt, ob eine E-Mail Spam ist. Dazu wird die E-Mail-Herkunft, der Inhalt der Nachricht und deren Transportweg analysiert.	Ja
Directory Harvesting	Das Modul stoppt E-Mails, die nach dem Zufallsprinzip erzeugt an einen Server gesendet werden, für die aber meist keine Benutzer existieren.	Ja
Phishing	Dieser Filter blockiert E-Mails, die Links in den Nachrichtentexten enthalten, die auf bekannte Phishing-Sites zeigen oder typische Phishing-Keywords enthalten.	Ja
Sender Policy Framework	Dieser Filter stoppt E-Mails, die von Domänen stammen, die in den SPF-Records nicht autorisiert wurden.	Nein
Auto-Whitelist	Wenn an diese Adressen eine E-Mail gesendet wird, werden Spam-Filter automatisch ignoriert.	Ja
Whitelists	Eine benutzerdefinierte Liste sicherer E-Mail-Adressen	Ja
Email Blacklist	Eine benutzerdefinierte Liste gesperrter E-Mail-Nutzer oder Domänen.	Ja
DNS-Blacklists	Prüft, ob die empfangene E-Mail von Absendern stammt, die in einer öffentlichen DNS-Blacklist bekannter Spammer enthalten sind.	Ja
Spam URI Realtime Blocklists	Dieser Filter stoppt E-Mails, die Links zu Domänen enthalten, die in den öffentlichen Spam-URL-Blocklists enthalten sind, beispielsweise sc.surbl.org.	Ja
Header-Prufüng	Dieses Modul analysiert die einzelnen Felder im Header durch Vergleich mit dem SMTP- und MIME-Feld.	Ja

Keyword-Prufüng	Spam-Mails werden anhand gesperrter Keywords in der E-Mail-Überschrift oder in der E-Mail-Nachricht identifiziert.	Nein
Neue Absender	E-Mails, die von Absendern stammen, an die noch nie eine E-Mail gesendet wurde.	Nein
Bayes'sche Analyse	Ein Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.	Nein

Wie aus der Tabelle oben zu ersehen, sind nicht alle Spam-Filter standardmäßig aktiviert. Dies hängt damit zusammen, dass die Konfigurationseinstellungen netzwerk- und infrastrukturabhängig sind und daher nicht voreingestellt werden können. Obgleich wichtige Filter wie SpamRazer standardmäßig aktiviert sind, sollten Sie nach der Installation von GFI MailEssentials die übrigen Spam-Filter und Filtermechanismen prüfen und aktivieren. Weitere Informationen finden Sie unter Spam-Filter dieses Handbuchs auf Seite 40 in diesem Handbuch.

Spam-Aktionen

Durch die Spam-Filter können bei Erkennung einer Spam-Mail verschiedene Aktionen ausgelöst werden. Diese Aktionen legen fest, wie mit der erkannten Spam-Mail verfahren wird; Sie können sie für jeden einzelnen Filter konfigurieren. Unterstützte Spam-Filter-Aktionen sind:

- Spam-Mail kennzeichnen (Standardvorgabe)
- Spam-Mail in einen zentralen Ordner verschieben
- Spam-Mail in öffentliche Ordner verschieben
- Spam-Mail in den Junk-Ordner verschieben
- Spam-Mail an eine bestimmte E-Mail-Adresse weiterleiten
- Spam-Mail löschen

Standard-Spamaktionen

Die Standardaktion, die durchgeführt wird, wenn GFI MailEssentials eine Spam-E-Mail blockiert, hängt vom Ort der Installation der Software ab:

Installation	Standardmaßnahme	Beschreibung
GFI MailEssentials ist auf demselben Computer wie Microsoft Exchange installiert.	E-Mail wird in den Unterordner des Exchange-Postfachs verschoben.	Wenn ein Filter eine Spam-E-Mail blockiert, wird die E-Mail in einen Unterordner im Posteingang mit der Bezeichnung „Vermutliche Spam" verschoben.
GFI MailEssentials ist nicht auf demselben Rechner wie Microsoft Exchange installiert.	Kennzeichnung	Spamfilter ergänzt Präfix [SPAM] im Betreff-Feld der E-Mails. Gekennzeichnete E-Mails werden immer noch in den Posteingang des Benutzers geleitet.

Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

2.2 Spam an einen besonderen Spam-Ordner umleiten

Um Spam-Mails aus den Empfängerpostfächern zu filtern, konfigurieren Sie GFI MailEssentials so, dass die E-Mails in besondere Spam-Ordner umgeleitet werden. Sie können für jeden Spam-Filter einen anderen Spam-Ordner konfigurieren. Auf diese Weise können Sie die Spam-Mails in Kategorien zusammenfassen; dadurch bleibt transparent, welcher Filter Ihre Spam-Mail herausgefiltert hat. Diese Transparenz ist wichtig, wenn Sie falsch-positive Treffer identifizieren und Ihre Filter verfeinern wollen.

Spam-Mail-Umleitung in Ordner aktivieren

Je nach Ihrer Konfiguration sind verschiedene Spam-Filter-Aktionen zum Verschieben in besondere Ordner verfügbar.

Wenn Sie eine Infrastruktur mit Microsoft Exchange 2003/2007/2010 einsetzen, können Spam-Mails mit folgenden Aktionen in Ordner verschoben werden:

- **Im Posteingang** - Mit dieser Option leiten Sie die Spam-Mails in den Posteingang des Benutzers um.
- **In Exchange-Junk-Ordner des Benutzers verschieben** - Mit dieser Option verschieben Sie alle Spam-Mails in den Standard-Junk-Ordner des Benutzers.
- **In den Exchange Postfach-Unterordner** - Mit dieser Option leiten Sie alle Spams in einen bestimmten Ordner des Benutzerpostfachs um.

Bei anderen Infrastrukturlösungen kann der Benutzer Spam-Mails in einen besonderen Ordner des Clients/Endbenutzers umleiten.

2.2.1 Konfigurieren der E-Mail-Umleitung in Ordner

HINWEIS: Dieser Abschnitt betrifft nur GFI MailEssentials bei Installation auf einem Microsoft Exchange Server. Wenn GFI MailEssentials auf einem separaten Rechner installiert ist, verfahren Sie entsprechend dem Abschnitt Verschieben vom Spam-E-Mails in die Postfachordner des Benutzers auf Seite 127 in diesem Handbuch

1. Starten Sie die Konfigurationskonsole für GFI MailEssentials, indem Sie auf folgende Optionen klicken:

Start ► Alle Programme ► GFI MailEssentials ► GFI MailEssentials Configuration.

2. Klicken Sie in der Liste der Filter im Knoten **Anti-Spam** mit der rechten Maustaste auf den Filter, den Sie konfigurieren wollen, **z. B. Header Prüfung,** und dann auf **Eigenschaften**.

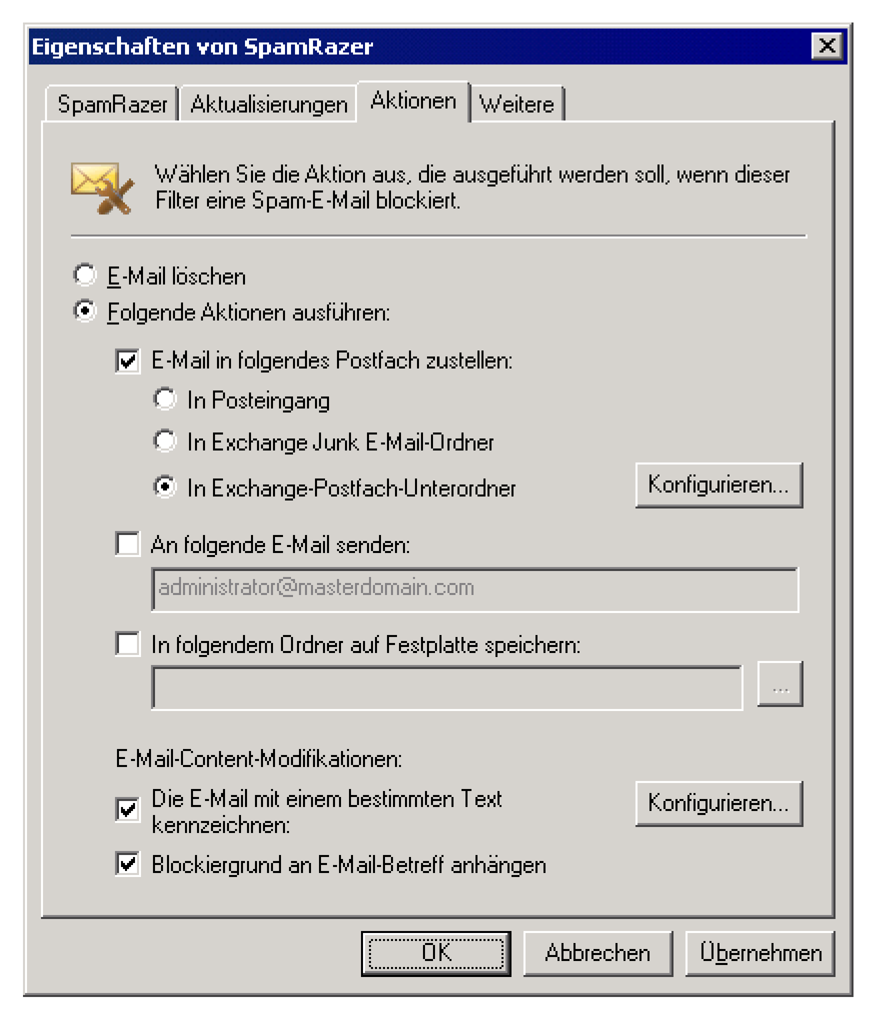


Bild 1 - Konfiguration der gewünschten Aktion

3. Klicken Sie auf die Registerkarte **Aktionen** um auf die Optionen für die Konfiguration der Spam-Filter-Aktionen zuzugreifen

4. Wählen Sie die Option "**E-Mail in Postfach speichern**" und klicken Sie auf eine der folgenden Optionen:

- **Im Posteingang** - Mit dieser Option leiten Sie die Spam-Mails in den Posteingang des Benutzers um.
- **In Exchange-Junk-Ordner des Benutzers verschieben** - Mit dieser Option verschieben Sie alle Spam-Mails in den Standard-Junk-Ordner des Benutzers.
- **In den Exchange Postfach-Unterordner** - Mit dieser Option leiten Sie alle Spams in einen bestimmten Ordner des Benutzerpostfachs um. Klicken Sie auf **Konfigurieren**, um den Dialog **In Exchange-Ordner verschieben** zu öffnen und den Ordner einzugeben, in den die Spam- E-Mail verschoben werden soll.

  Beispiel: Die Option "Posteingang\Spam E-Mail" erstellt im Posteingang einen Unterordner mit der Bezeichnung "Spam E-Mail".

5. Klicken Sie auf **OK** um Ihre Konfiguration zu speichern.

6. Wiederholen Sie dies für alle aktivierten Spamfilter.

2.3 Scannen öffentlicher Ordner aktivieren

Die Spammer entwickeln ihre Verfahren laufend weiter, daher kommt es immer wieder vor, dass Spam-Mails von Spam-Filtern nicht erkannt werden und ins Postfach des Empfängers gelangen. Durch das Scannen öffentlicher Ordner können die Benutzer manuell E-Mails als Spam kennzeichnen und die Spam-Filter von GFI MailEssentials trainieren, damit ähnliche E-Mails als Spam erkannt werden.

Beim Scannen öffentlicher Ordner lädt GFI MailEssentials E-Mails aus den öffentlichen Ordnern und ergänzt diese in der Whiteliste/Blacklist sowie in der HAM/SPAM-Datenbank. Bei Systemen mit Microsoft Exchange Server oder Lotus Domino werden öffentliche Ordner automatisch nach Abschluss der Konfiguration erstellt.

Führen Sie die in den folgenden Abschnitten aufgeführten Anweisungen aus um das Scannen öffentlicher Ordner zu aktivieren.

2.3.1 Konfiguration des Scannens öffentlicher Ordner für Microsoft Exchange Server

1. Klicken Sie in der Konfigurationskonsole für GFI MailEssentials mit der rechten Maustaste auf den Knoten **Anti-Spam ► Anti-Spam Einstellungen** und wählen Sie die Option **Eigenschaften**.

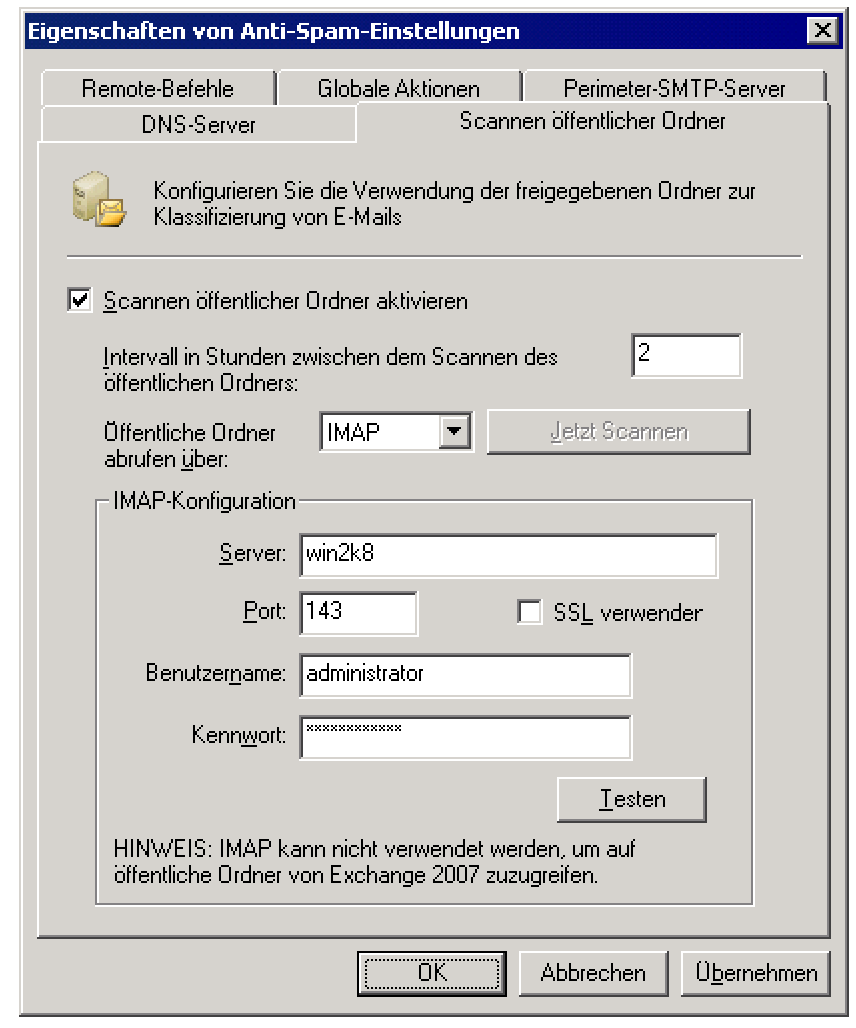


Bild 2 - Konfiguration des Scannens öffentlicher Ordner

2. Klicken Sie auf die Registerkarte **Scannen öffentlicher Ordner** und dann in das Kontrollkästchen **Scannen öffentlicher Ordner** aktivieren.

3. Wählen Sie aus der Anzeigeliste **Öffentliche Ordner abrufen über** das Verfahren aus, mit dem GFI MailEssentials die E-Mails aus öffentlichen Ordnern holen soll.

- **Für Exchange Server 2000/2003 -** Wählen Sie MAPI, IMAP oder WebDAV.
- **Für Exchange Server 2007 -** Wählen Sie WebDAV oder Web Services.
- **Für Exchange Server 2010 -** Wählen Sie Web Services.

Verfügbare Optionen:

- **MAPI** - Damit MAPI verwendet werden kann, muss GFI MailEssentials auf dem Computer installiert sein, auf dem auch Microsoft Exchange Server installiert ist. Weitere Einstellungen sind nicht erforderlich.
- **IMAP** - Erfordert Microsoft Exchanges IMAP-Service. IMAP erlaubt ein Scannen öffentlicher Ordner aus der Ferne und arbeitet bei Umgebungen mit Firewalls ausgezeichnet. Außerdem kann IMAP auch bei anderen Mailservern eingesetzt werden, die IMAP unterstützen. Benötigte Parameter:
  - Mail-Servername
  - Portnummer (Standard-IMAP-Port ist 143)
  - Benutzername/Kennwort
  - Wählen Sie für eine sichere Verbindung die Option **SSL verwenden**.
- **WebDAV** - Geben Sie den Namen des Mailservers, den Port (Standardport für WebDAV ist 80), den Benutzernamen, das Kennwort und die Domäne ein. Markieren Sie für eine sichere Verbindung das Kontrollkästchen **SSL verwenden**. Standardmäßig sind öffentliche Ordner in dem virtuellen Verzeichnis 'public' erreichbar. Wenn diese Einstellung verändert wurde, geben Sie den korrekten Namen des virtuellen Verzeichnisses ein um auf die öffentlichen Ordner zuzugreifen; bearbeiten Sie dazu den Text in dem Feld URL.
- **Web Services** - Geben Sie den Namen des Mailservers, den Port (Standardport für Web Services ist 80), den Benutzernamen, das Kennwort und die Domäne ein. Markieren Sie für eine sichere Verbindung das Kontrollkästchen **SSL verwenden**. Standardmäßig sind öffentliche Ordner in dem virtuellen Verzeichnis 'public' erreichbar. Wenn diese Einstellung verändert wurde, geben Sie den korrekten Namen des virtuellen Verzeichnisses ein um auf die öffentlichen Ordner zuzugreifen; bearbeiten Sie dazu den Text in dem Feld URL.



Bild 3 - Test zum Scannen öffentlicher Ordner erfolgreich.

4. Klicken Sie auf **Jetzt scannen** um automatisch öffentliche Ordner zu erstellen.

5. Klicken Sie auf **Testen**, wenn Sie IMAP WebDAV oder Web Services konfigurieren. Sie erhalten auf dem Bildschirm einen Hinweis über Erfolg oder Misserfolg. Wenn der Test fehlschlägt, überprüfen/aktualisieren Sie die Authentifizierungsdaten und versuchen Sie es erneut.

2.3.2 Konfigurieren eines dezidierten Benutzerkontos für Exchange Server 2000/3

Wenn GFI MailEssentials in einer DMZ installiert ist, sollten Sie aus Sicherheitsgründen unbedingt ein dezidiertes Benutzerkonto erstellen um E-Mails aus öffentlichen Ordnern zu laden und zu scannen. Die Benutzer haben Zugriff auf die GFI-Spam-Ordner.

1. Erstellen Sie einen neuen Active Directory (AD-) Benutzer mit Poweruser-Rechten.

2. Öffnen Sie im Microsoft Exchange System Manager den Knoten **Ordner ► Öffentliche Ordner**.

3. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **Anti-Spam folders** und dann auf **Eigenschaften**.

4. Klicken Sie auf die Registerkarte **Berechtigungen** und wählen Sie **Client-Berechtigungen** aus.

5. Klicken Sie auf **Hinzufügen …**, wählen Sie die Option "Neuer Benutzer" und klicken Sie auf **OK**.

6. Wählen Sie die Option "Neuer Benutzer" aus der Liste der Client-Berechtigungen und aus der angezeigten Liste die Rolle 'Besitzer'. Achten Sie darauf, dass alle Kontrollkästchen aktiviert sind und die Radioschaltflächen auf **Alle** eingestellt sind.

7. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8. Klicken Sie im Microsoft Exchange System Manager mit der rechten Maustaste auf **Anti-Spam folders** und dann auf **Alle Aufgaben ► Einstellungen übernehmen**.

9. Klicken Sie auf die Option **Ordnerrechte** und dann auf **OK**.

10. Definieren Sie die Authentifizierungsdaten des in Schritt 1 erstellten Poweruser-Kontos und testen Sie die Konfiguration um sicherzugehen, dass die Rechte richtig definiert sind.

2.3.3 Konfigurieren eines dezidierten Benutzerkontos für Exchange Server 2007/2010

Wenn Sie ein dezidiertes Benutzerkonto konfigurieren, das E-Mails

aus den öffentlichen GFI-Spam-Ordnern laden soll, muss der Benutzer Zugriffsrechte als 'Besitzer' der öffentlichen GFI-Anti-Spam folders haben.

1. Erstellen Sie einen neuen Active Directory (AD) (Power-) User.

2. Melden Sie sich bei Microsoft Exchange Server mit Administratorrechten an.

3. Öffnen Sie die 'Microsoft Exchange Manager Shell' und geben Sie folgenden Befehl ein:

```
Get-PublicFolder -Identity "\GFI Anti-Spam Folders" -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User "BENUTZERNAME" -AccessRights owner -Server "SERVERNAME"}
```

4. Ändern Sie "BENUTZERNAME" und "SERVERNAME" entsprechend dem betreffenden Active Directory-Benutzer.

- Beispiel:

```
Get-PublicFolder -Identity "\GFI Anti-Spam Folders" -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User "mesuser" -AccessRights owner -Server "exch07"}
```

2.3.4 Verbergen von Benutzermitteilungen in GFI-Spam-Ordnern

Aus Sicherheits- und Datenschutzgründen sollten Sie die Benutzernachrichten verbergen, die sich in einem GFI-Spam-Ordner befinden. So können die Benutzer Nachrichten an die Ordner senden, aber die vorhandenen Nachrichten nicht sehen (nicht einmal die, die sie selbst gesendet haben). Um Benutzerrechte zu konfigurieren und Nachrichten für unbefugte Benutzer zu verbergen, gehen Sie wie folgt vor:

1. Öffnen Sie im Microsoft Exchange System Manager den Knoten **Ordner ► Öffentliche Ordner.**

2. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **Anti-Spam folders** und dann auf **Eigenschaften**.

3. Klicken Sie auf die Registerkarte **Berechtigungen** und dann auf **Client-Berechtigungen**.

4. Klicken Sie auf **Hinzufügen…** und wählen Sie den Benutzer/die Gruppe aus, deren Nachrichten Sie verbergen wollen, und klicken Sie dann auf **OK**.

5. Wählen Sie den zuvor konfigurierten Benutzer/die Benutzergruppe für die Client-Berechtigungsliste aus und stellen Sie als Benutzerrolle **Teilnehmen** ein.

6. Achten Sie darauf, dass nur das Kontrollkästchen **Elemente erstellen** ausgewählt ist und die Radioschaltflächen auf **Keine** eingestellt sind.

7. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8. Klicken Sie im Microsoft Exchange System Manager mit der rechten Maustaste auf **Anti-Spam folders** und dann auf **Alle Aufgaben ► Einstellungen übernehmen**.

9. Aktivieren Sie das Kontrollkästchen **Ordnerrechte** und klicken Sie auf **OK**.

2.3.5 Konfiguration zum Konfiguration zum Scannen öffentlicher Ordner für Lotus Domino Server

Schritt 1: Erstellen Sie eine neue Datenbank, in der Sie die öffentlichen Ordner von GFI MailEssentials speichern wollen.

1. Klicken Sie in IBM Domino Administrator auf **Datei ► Datenbank ► Neu**.

2. Geben Sie für die neue Datenbank folgende Details ein:

- Server: <*Die Details Ihres Domino Servers*>
- Titel: Öffentlicher Order
- Dateiname: Public-F.nsf
- Wählen Sie als Vorlage für die neue Datenbank 'Mail (R7)'.

3. Klicken Sie auf **OK** um die Datenbank zu erstellen.

Schritt 2: Konvertieren Sie das Datenbankformat der neu erstellten Datenbank.

1. Klicken Sie in der Lotus Domino Server Console, und geben Sie folgenden Befehl ein:

```
Load Convert -e -h <Datenbank Dateiname>
```

- Beispiel:

```
Load Convert -e -h Public-F.nsf
```

Schritt 3: Erstellen Sie eine neue Mail-In-Datenbank:

Sie müssen ein neues Postfach erstellen, damit Sie den neuen öffentlichen Ordner von GFI MailEssentials speichern können.

1. Wählen Sie im IBM Domino Administrator die Registerkarte **Personen und Gruppen** und klicken Sie auf **Mail-In-Datenbanken und Ressourcen**.

2. Klicken Sie auf **Mail-In-Datenbank hinzufügen** und geben Sie die neue Mail-In-Datenbank wie folgt ein:

- Name der Mail-In-Datenbank: Public Folders
- Beschreibung: GFI MailEssentials-Postfach
- Internetadresse: <*public@<yourdomain>.com*>
- Internetnachricht: 'Keine Präferenz'
- Eingehende E-Mail verschlüsseln: 'Nein'
- Domäne: <*yourdomain*>
- Server: <*Name Ihres Domino Servers*>
- Dateiname: 'Public-F.nsf'

HINWEIS: Sie müssen mit der oben erstellten Mail-In-Datenbank einen Benutzer verknüpfen. Dieses Konto wird vom GFI MailEssentials-Server für den Verbindungsaufbau mit Lotus Domino-Server verwendet.

Schritt 4: Konfigurieren Sie GFI MailEssentials.

Definieren Sie den gemeinsamen Namespace, der beim Verbindungsaufbau mit dem Lotus Domino IMAP-Service verwendet wird:

1. Klicken Sie auf **Start ► Ausführen** und geben Sie **Regedit** ein.

2. Suchen Sie folgenden Registrierschlüssel:

`<HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME14\Attendant\rpfolders:8\>`

3. Erstellen Sie folgende Schlüssel:

- Name: 'FolderDelimiter'
- Typ: STRING
- Wert: '\\'

- Name: 'SharedNamespace'
- Typ: STRING
- Wert: <Präfixbezeichnung des öffentlichen Ordners\Name der neuen Mail-In-Datenbank\>

Laden Sie die Werte für den Schlüssel 'sharednamespace' wie folgt:

- **Präfix für öffentlichen Ordner, Name**

  1. Klicken Sie in IBM Domino Administrator auf die Registerkarte **Konfiguration**.

  2. Klicken Sie auf **Server ► Konfigurationen,** dann auf den Domino Server sowie auf **Konfiguration bearbeiten.**

  3. Wählen Sie auf der Registerkarte **IMAP** die Registerkarte **Öffentliche Ordner und Ordner anderer Benutzer**. Den 'Public Folder Prefix' finden Sie im Abschnitt "Public Folder".

  Name der Mail-In-Datenbank

  1. Wählen Sie in IBM Domino Administrator die Registerkarte **Personen und Gruppen**.

  2. Klicken Sie auf den Knoten **Mail-In-Datenbanken und Ressourcen**. Der Name der neuen Mail-In-Datenbank wird im rechten Feld angezeigt.

Schritt 5: Starten Sie den IMAP-Service auf Domino Server neu.

1. Öffnen Sie die Konsole von Lotus Notes.

2. Geben Sie 'tell imap quit' ein und warten Sie, bis die Aufgabe abgeschlossen ist.

3. Sobald diese Schritte abgeschlossen sind, geben Sie 'load imap'ein.

Schritt 6: Konfigurieren Sie GFI MailEssentials.

Konfigurieren Sie die Scan-Eigenschaften für den öffentlichen Ordner von GFI MailEssentials. 1. Klicken Sie in der Konfiguration von GFI MailEssentials auf den Knoten **Anti-Spam** und dann auf **Eigenschaften.**

2. Wählen Sie die Registerkarte **Scannen öffentlicher Ordner** aus und geben Sie folgende Werte ein:

- Server: *<IP-Adresse des Domino Server>*
- Port: 143 (Standard)
- Benutzername: Den mit der Mail-In-Datenbank verknüpften Benutzernamen
- Kennwort: Benutzerkennwort

3. Testen Sie die Konfiguration, indem Sie auf die Schaltfläche **Testen** klicken und anschließend auf **Jetzt scannen** um die öffentlichen Ordner zu erzeugen.

Schritt 7: Kontrollieren Sie, ob die öffentlichen Ordner erstellt werden.

Prüfen Sie mit Telnet, ob die öffentlichen Ordner erfolgreich erstellt wurden:

1. Öffnen Sie auf dem Computer mit GFI MailEssentials eine Befehlszeile.

2. Geben Sie ein: 'telnet'

3. Geben Sie ein: 'Open <*IP-ADRESSE*> 143'

4. Geben Sie ein: 'ao1 login <public@yourdomain.com> <Kennwort>'

5. Geben Sie ein: 'ao5 list “<Präfix des öffentlichen Orders\Name der neuen Mail-In-Datenbank\>” “*”.

6. Die Ausgabe des oben erwähnten Befehls sollte die öffentlichen Ordner wie in dem folgenden Bild anzeigen:

```
Telnet 127.0.0.1
ao5 list "public folders\public-folder" "*"
* LIST (\HasChildren) "\\" {48}
Public Folderspublic-folder\GFI AntiSpam-Ordner
* LIST (\HasChildren) "\\" {65}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Zur Blacklist hinzufugen
* LIST (\HasNoChildren) "\\" {75}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Zur Blacklist hinzufugen\Bearbeitet
* LIST (\HasChildren) "\\" {65}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Zur Whitelist hinzufugen
* LIST (\HasNoChildren) "\\" {75}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Zur Whitelist hinzufugen\Bearbeitet
* LIST (\HasChildren) "\\" {76}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Ich mochte diese Diskussionsliste
* LIST (\HasNoChildren) "\\" {86}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Ich mochte diese Diskussionsliste\Bearbeitet
* LIST (\HasChildren) "\\" {73}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Diese E-Mail ist kein Spam
* LIST (\HasNoChildren) "\\" {83}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Diese E-Mail ist kein Spam\Bearbeitet
* LIST (\HasChildren) "\\" {67}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Diese E-Mail ist Spam
* LIST (\HasNoChildren) "\\" {77}
Public Folderspublic-folder\GFI AntiSpam-Ordner\Diese E-Mail ist Spam\Bearbeitet
```

7. Geben Sie 'ao3 logout' ein.

HINWEIS: Entfernen Sie mit Lotus Notes Designer unerwünschte Ansichten und Formulare aus der zuvor erstellten Datenbank.

3 Routineadministration

3.1 Prüfung von Spam-Mails

3.1.1 Ablauf der Spamprüfung

- Weisen Sie die einzelnen E-Mail-Benutzer darauf hin, dass sie Spam-Mails regelmäßig kontrollieren sollten.
- Wenn zulässige E-Mails fälschlicherweise als identifiziert werden (falsch-positive Treffer), informieren Sie sich bitte im Abschnitt Umgang mit zulässigen E-Mails, wie Sie GFI MailEssentials einstellen, damit ähnliche E-Mails nicht als Spam klassifiziert werden.
- Falls E-Mails fälschlicherweise nicht als Spam identifiziert werden, schlagen Sie im Abschnitt Umgang mit Spam nach, wie Sie GFI MailEssentials einstellen müssen, damit ähnliche E-Mails als Spam klassifiziert werden.

3.2 Umgang mit zulässigen E-Mails

Wie jede Anti-Spam-Lösung braucht auch GFI MailEssentials eine gewisse Zeit, bis die optimale Spam-Filterbedingungen eingestellt sind. Solange dies noch nicht der Fall ist, ist es möglich, dass zulässige E-Mails als Spam identifiziert werden.

In solchen Fällen sollten die Benutzer E-Mails, die fälschlicherweise als Spam identifiziert wurden, in den Ordner 'Zur Whitelist hinzufügen' bzw. in den Ordner 'Dies ist eine zulässige E-Mail' schieben, damit GFI MailEssentials 'lernt', dass die betreffende E-Mail keine Spam-Mail ist.

Wichtige Hinweise

In Microsoft Outlook verschieben Sie E-Mails per Drag&Drop in den gewünschten Ordner. Um eine Kopie der E-Mail zu behalten, halten Sie die Taste **STRG** gedrückt um die E-Mail zu kopieren und nicht nur zu verschieben.

3.2.1 Hinzufügen von Absendern oder Newslettern zur Whitelist.

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI Anti-Spam-Ordner ► Zur Whitelist hinzufügen**.

2. Schieben Sie per Drag&Drop E-Mails oder Newsletter in den öffentlichen Ordner **Zur Whitelist hinzufügen**.

3.2.2 Hinzufügen von Diskussionslisten zur Whitelist

Diskussionslisten **(KEINE Newsletter)** werden oft ohne die Empfänger-E-Mail-Adresse in dem Feld MIME TO versendet und daher als Spam gekennzeichnet. Um solche Diskussionslisten zu empfangen, schieben Sie die E-Mail-Adressen dieser gültigen Listenabsender in die Whitelist.

Diskussionslisten in der Whitelist hinzufügen

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI AntiSpam-Ordner ► Ich möchte diese Diskussionsliste**.

2. Schieben Sie Diskussionslisten per Drag&Drop in den öffentlichen Ordner **Ich möchte diese Diskussionsliste**.

3.2.3 HAM zur Datenbank zulässiger E-Mails zulässige E-Mails hinzufügen.

1. Suchen Sie unter den öffentlichen **GFI AntiSpam-Ordner ► Diese E-Mail ist kein Spam**.

2. Schieben Sie die E-Mails per Drag&Drop in den öffentlichen Ordner **Diese E-Mail ist kein Spam**.

3.3 Umgang mit Spam-Mails

Wenn GFI MailEssentials beginnt, Spam-Mails mit der Standardinstallation zu identifizieren, kann es Fälle geben, in denen Spam-Mails unerkannt in das Benutzerpostfach gelangen. In der Regel kommt dies vor, weil Konfigurationseinstellungen noch nicht definiert wurden oder weil es sich um eine neue Form von Spam-Mails handelt, die GFI MailEssentials noch nicht kennt. In beiden Fällen beseitigen Sie solche Situationen, wenn Sie GFI MailEssentials so konfigurieren, dass diese Spam-Mails zurückgehalten werden.

HINWEIS: Wie Sie Probleme im Zusammenhang mit E-Mails lösen, die nicht als Spam erkannt wurden, finden Sie in dem Kapitel Problembehandlung und Support auf Seite 133 in diesem Handbuch.

Die Benutzer sollten in solchen Fällen diese E-Mails in die Ordner 'Zur Blacklist hinzufügen' und 'Diese E-Mail ist Spam' verschieben, damit GFI MailEssentials 'lernt', dass die betreffende E-Mail eine Spam-Mail ist.

Wichtige Hinweise

1. In Microsoft Outlook verschieben Sie E-Mails per Drag&Drop in den gewünschten Ordner. Um eine Kopie der E-Mail zu behalten, halten Sie die Taste **STRG** gedrückt um die E-Mail zu kopieren und nicht nur zu verschieben.

2. Weitere Informationen, wie Sie automatisch die GFI Anti-Spam Ordner erstellen, finden Sie unter Scannen öffentlicher Ordner aktivieren auf Seite 7 in diesem Handbuch.

3.3.1 Hinzufügen von Absendern zur Blacklist

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI AntiSpam-Ordner ► Zur Blacklist hinzufügen**.

2. Verschieben Sie per Drag&Drop E-Mails in den öffentlichen Ordner **Zur Blacklist hinzufügen**.

3.3.2 Hinzufügen von Spam-Mails zur Spam-Datenbank

1. Suchen Sie unter den öffentlichen Ordnern den **GFI AntiSpam-Ordner ► Diese E-Mail ist Spam**.

2. Verschieben Sie die Spam-Mail per Drag&Drop in den öffentlichen Ordner 'Diese E-Mail ist Spam'.

3.4 Anzeige des Spam-Status auf dem Dashboard

Das GFI MailEssentials-Dashboard zeigt den Status Ihres Anti-Spam-Systems einschließlich der Bearbeitung der E-Mails und der Statistik. Das Dashboard von GFI MailEssentials nutzen Sie wie folgt:

1. Klicken Sie auf **Start ► Alle Programme ► GFI MailEssentials ► GFI MailEssentials Dashboard**.

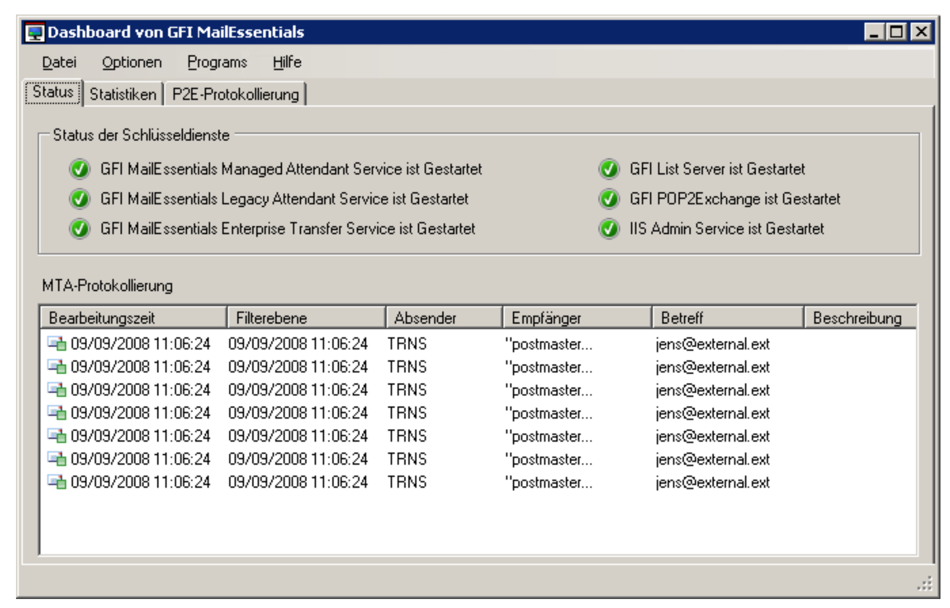


Bild 4 - GFI MailEssentials Dashboard

2. Klicken Sie auf folgende Optionen:

- **Status,** um den Status der GFI MailEssentials-Services und die E-Mail-Bearbeitungsaktivität anzuzeigen.
- **Statistik** um statistische Übersichten zum E-Mail-Durchsatz und zu den von allen Spam-Filtern geblockten Spam-Mails sowie Zahlenangaben zu den eingehenden und ausgehenden E-Mails und Spam-Mails anzuzeigen.
- **P2E Logging:** um ein Protokoll der POP2-Exchange-Aktivitäten anzuzeigen.

HINWEIS: Weitere Informationen zu POP2-Exchange finden Sie im Abschnitt Konfiguration von POP3 und Download-Einwahlverbindung auf Seite 103 in diesem Handbuch.

3.5 Erzeugen von Spam-Berichten

Der Spam-Bericht ist ein Kurzbericht, der dem Benutzer oder Administrator per E-Mail gesendet wird. Dieser Bericht führt die Gesamtzahl der von GFI MailEssentials verarbeiteten E-Mails sowie die Zahl der geblockten Spam-Mails innerhalb eines bestimmten Zeitraums auf (… in der Regel seit dem letzten Spam-Bericht).

3.5.1 Konfigurieren von Spam-Berichten

Administrator-Spam-Bericht

1. Klicken Sie auf **Anti-Spam ► Spam-Bericht ► Eigenschaften**.

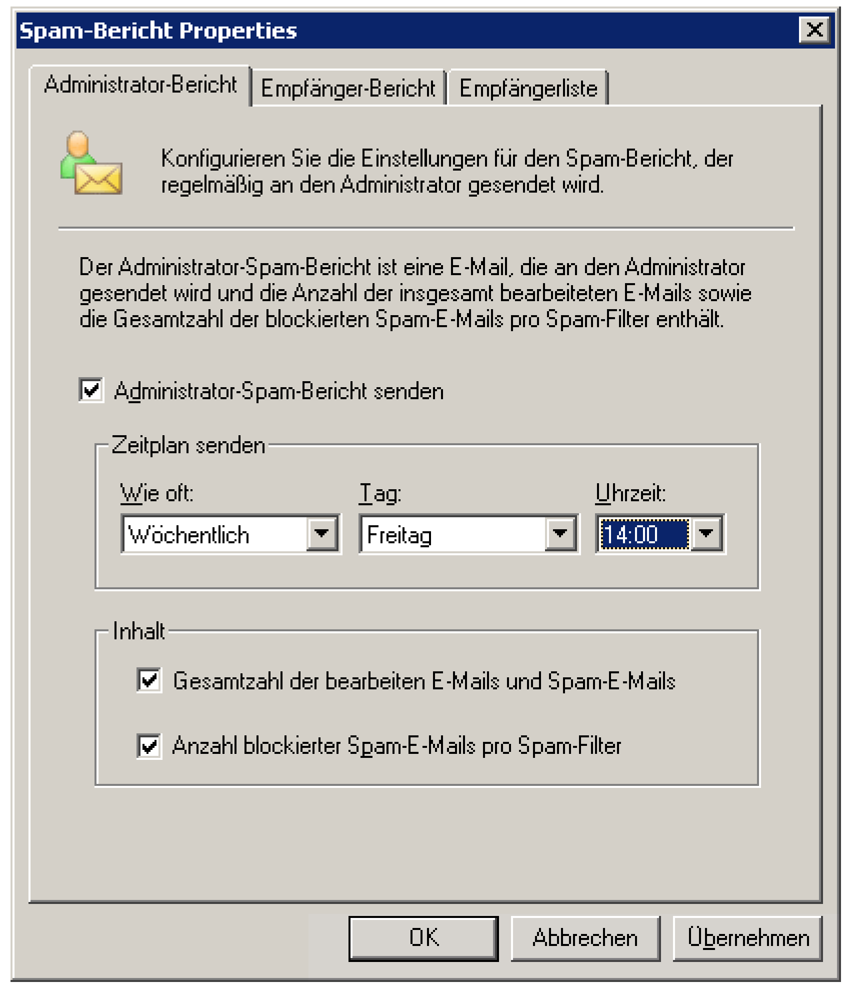


Bild 5 - Spam-Bericht-Eigenschaften/Administrator-Spam-Bericht

2. Klicken Sie auf der Registerkarte **Administrator-Bericht** auf **Administrator-Spam-Bericht senden** um den Spam-Bericht zu aktivieren**.**

3. Konfigurieren Sie die gewünschte Sendehäufigkeit (täglich, wöchentlich, monatlich) über die Dropdown-Liste **Sendezeitplan**.

4. Geben Sie an, welchen Inhalt der Spam-Bericht in der E-Mail haben soll, entweder die **Gesamtzahl der verarbeiteten E-Mails und Spam-Mails** oder die **Gesamtzahl der pro Spam-Filter geblockten Spam-Mails** oder beide Angaben.

5. Schließen Sie die Einstellungen ab, indem Sie auf **Übernehmen** und **OK** klicken.

Empfänger-Spam-Bericht

1. Klicken Sie auf **Anti-Spam ► Spam-Bericht ► Eigenschaften**.

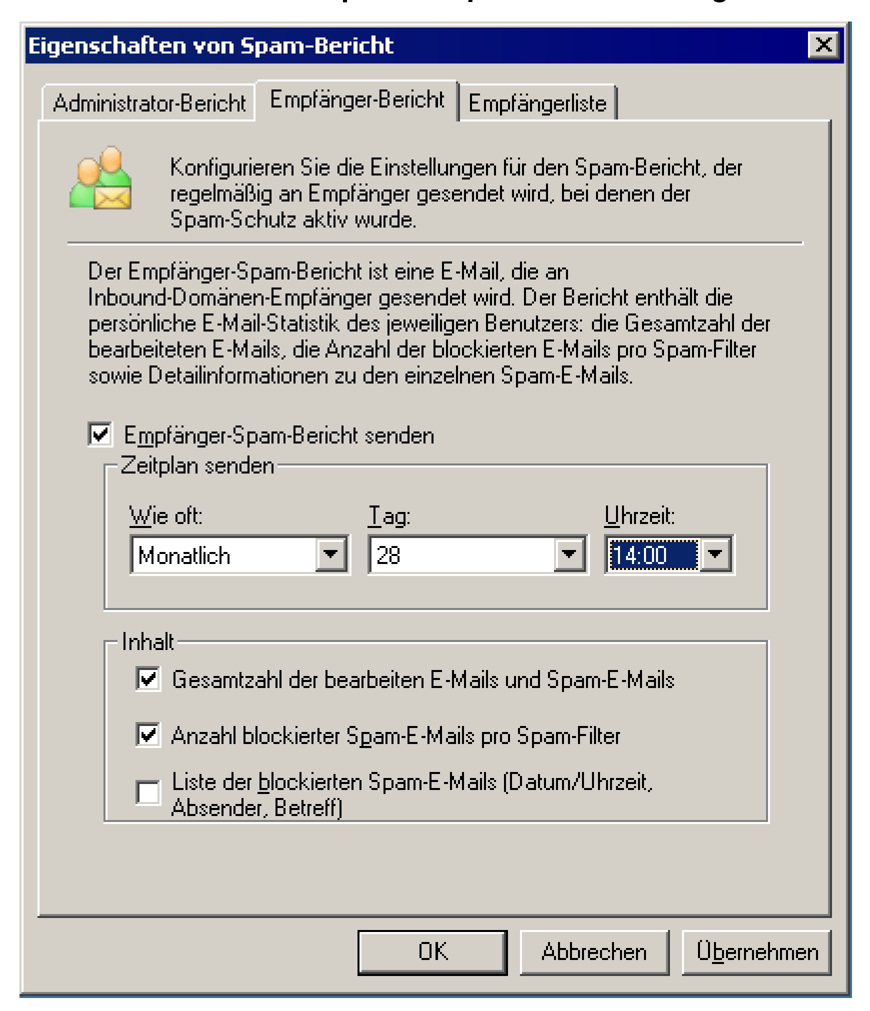


Bild 6 - Empfänger-Spam-Bericht

2. Klicken Sie auf der Registerkarte **Empfänger-Bericht** auf die Option **Empfänger Spam-Bericht senden** um einen Spam-Bericht zu aktivieren.

3. Konfigurieren Sie die gewünschte Sendehäufigkeit über die Option **Sendezeitplan**.

4. Legen Sie fest, was in dem in der E-Mail gesendeten Bericht enthalten sein soll:

- Gesamtzahl der verarbeiteten E-Mails und Spam-Mails
- Gesamtzahl der pro Spam-Filter geblockten Spam-Mails
- Liste der geblockten Spam-Mails

Oder eine beliebige Kombination dieser Optionen, je nach Bedarf.

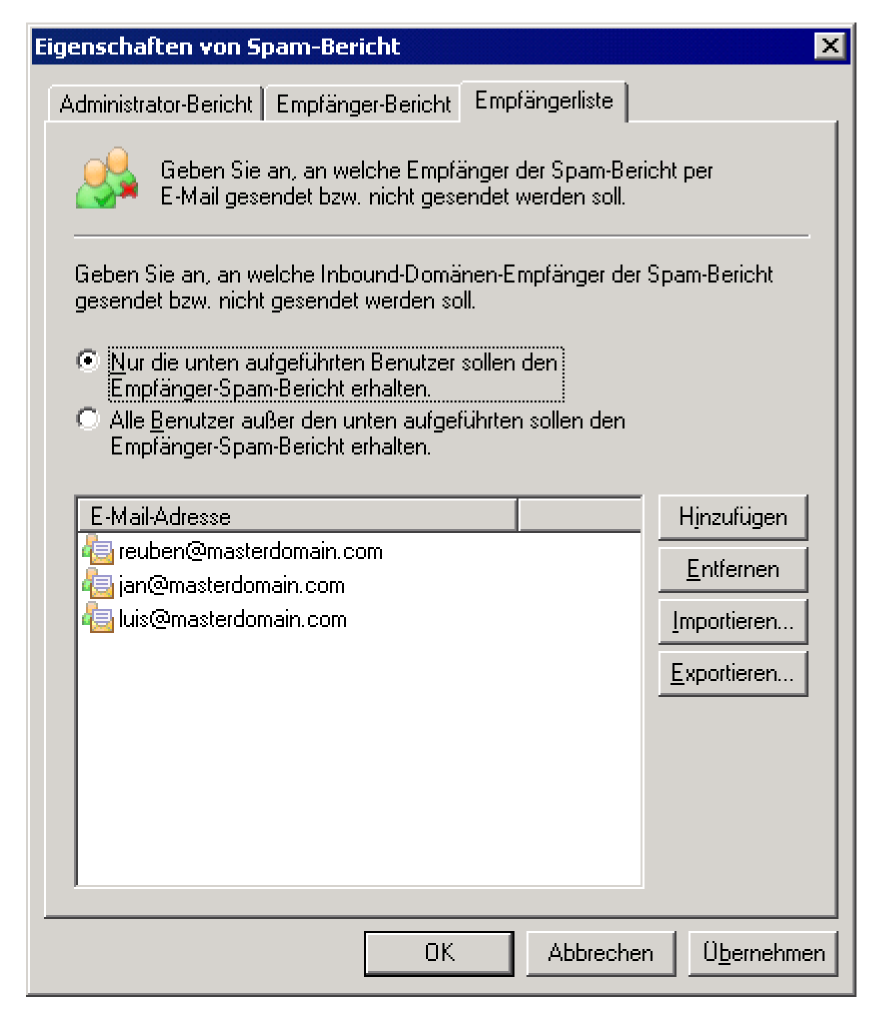


Bild 7 - Spam-Bericht-Empfängerliste

5. Klicken Sie auf die Registerkarte **Empfänger**, ergänzen Sie die Benutzer, die den Spam-Bericht erhalten sollen und wählen Sie aus, wie entschieden werden soll, wer den Spam-Bericht empfängt. Verfügbare Optionen:

- Nur die im Folgenden aufgelisteten Benutzer sollten einen Empfänger-Spam-Bericht erhalten.
- Alle Nutzer außer den im Folgenden aufgelisteten Benutzern erhalten den Empfänger-Spam-Bericht.

HINWEIS: Die benötigte Benutzerliste kann auch aus einer Datei im XML-Format importiert werden, wenn diese die gleiche Struktur besitzt, mit der GFI MailEssentials Daten exportiert.

6. Klicken Sie auf **Übernehmen** und **OK** um die Einstellungen abzuschließen.

3.6 Erstellen von E-Mail-Archiven

GFI MailEssentials besitzt eine Archivierungsfunktion, mit der die Aufbewahrung alter Datensätze Ihrer E-Mail-Nachrichten möglich ist. Da GFI MailEssentials eine Anti-Spam-Lösung ist, soll die integrierte Archivierungsfunktion nicht die Funktionalität umfangreicher E-Mail-Archiv-Lösungen wie GFI MailArchiver ersetzen oder duplizieren.

Zur Archivierung ist eine Datenbank erforderlich. GFI MailEssentials

unterstützt sowohl Microsoft Access als auch Microsoft SQL-Server.

Wichtige Hinweise

1. Interne E-Mails werden nicht archiviert.

2. Bei größeren Netzwerken empfehlen wir Microsoft SQL-Server.

3. Bei Microsoft Access ist die Größe der Datenbank auf 2 GB begrenzt. Bei MSDE und SQL-Server Express ist die Größe auf 2 bzw. 4 Gigabyte begrenzt.

4. Wenn die Microsoft Access-Datenbank eine Größe von 1 GB erreicht, wird eine E-Mail an den Administrator gesendet mit dem Hinweis, auf Microsoft SQL Server zu wechseln.

3.6.1 Aktivieren der Archivierung

1. Klicken Sie in der Konfigurationskonsole von GFI MailEssentials mit der rechten Maustaste auf **E-Mail-Management ► Mail-Archivierung** und dann auf **Eigenschaften**.

2. Klicken Sie auf die Registerkarte **Mail-Archivierung** und wählen Sie aus, ob Sie eingehende bzw. ausgehende E-Mails archivieren wollen.

3. Wählen und konfigurieren Sie das Archivierungsverfahren:

- **E-Mails in Textdatei archivieren** - archiviert eingehende und ausgehende E-Mails in separaten Textdateien für eingehende und ausgehende E-Mails. E-Mail-Anhänge werden nicht archiviert, wenn diese Option ausgewählt ist.
- **E-Mails in Datenbank archivieren** - archiviert alle E-Mails in einer Microsoft Access-Datenbank oder SQL/SQL-Server Express/MSDE-Datenbank. Bei dieser Option können E-Mail-Anhänge archiviert werden.

4. Um die Archivierung von E-Mails zu vermeiden, die von bestimmten Benutzern empfangen wurden, klicken Sie auf die Registerkarte **Ausnahmen**, markieren die Option **E-Mails nicht archivieren, wenn Absender oder Empfänger in der folgenden Liste enthalten ist**, klicken dann auf die Schaltfläche **Hinzufügen** und fügen die E-Mail-Adresse des Benutzers in der **E-Mail-Liste** hinzu.

5. Klicken Sie auf die Schaltfläche **OK** um die Konfiguration zu übernehmen.

3.6.2 Aktivieren des Archive Web Interface-Zugriffs über GFI MailEssentials

Wichtige Hinweise

Die Archiv Web-Schnittstelle (AWI) von GFI MailEssentials unterstützt keine 64 Bit-Betriebssysteme.

Installation von GFI MailEssentials Archive Web Interface (AWI) auf Microsoft IIS 7.0 (x86-Systeme)

Zur Installation von AWI auf Microsoft IIS 7.0 führen Sie folgende Schritte aus:

- Installieren Sie die ISS Web Server Rollendienste.

- Konfigurieren Sie die ISS Web-Anwendung, die durch AWI genutzt wird.

AWI benötigt folgende ISS Web-Server-Rollendienste zur einwandfreien Funktion:

- ASP
- Windows-Authentifizierung

So installieren Sie ISS Web-Server-Rollendienste auf Microsoft Windows 2008:

1. Öffnen Sie den 'Server-Manager'.

2. Öffnen Sie den Knoten **Rollen** und klicken Sie auf **Web-Server (IIS)**.

3. Klicken Sie auf der rechten Seite auf die Schaltfläche **Rollendienste hinzufügen**.

4. Wählen Sie die Rollendienste 'ASP' und 'Windows-Authentifizierung' und klicken Sie auf **Weiter**.

5. Klicken Sie auf die Schaltfläche **Installieren** um die Rollendienste zu installieren.

Konfigurieren Sie die IIS Web-Anwendung für AWI auf ISS 6.0

1. Starten Sie den Internet Services Manager, klicken Sie mit der rechten Maustaste auf den Knoten der Website und über das Popup-Menü auf **Neu ► Virtuelles Verzeichnis**. Der **Assistent zum Erstellen des virtuellen Verzeichnisses** wird angezeigt. Klicken Sie auf **Weiter** um fortzufahren.

2. Geben Sie einen Alias für das virtuelle Verzeichnis ein. In diesem Fall ist dies AWI, Sie können aber einen beliebigen Namen eingeben, solange er die Namenskonventionen für Ordner von Microsoft Windows erfüllt.

3. Sie müssen wissen, unter welchem Pfad Sie den Inhalt finden. Klicken Sie auf **Durchsuchen** und auf den Ordner AWI\wwwroot im Installationspfad von GFI MailEssentials.

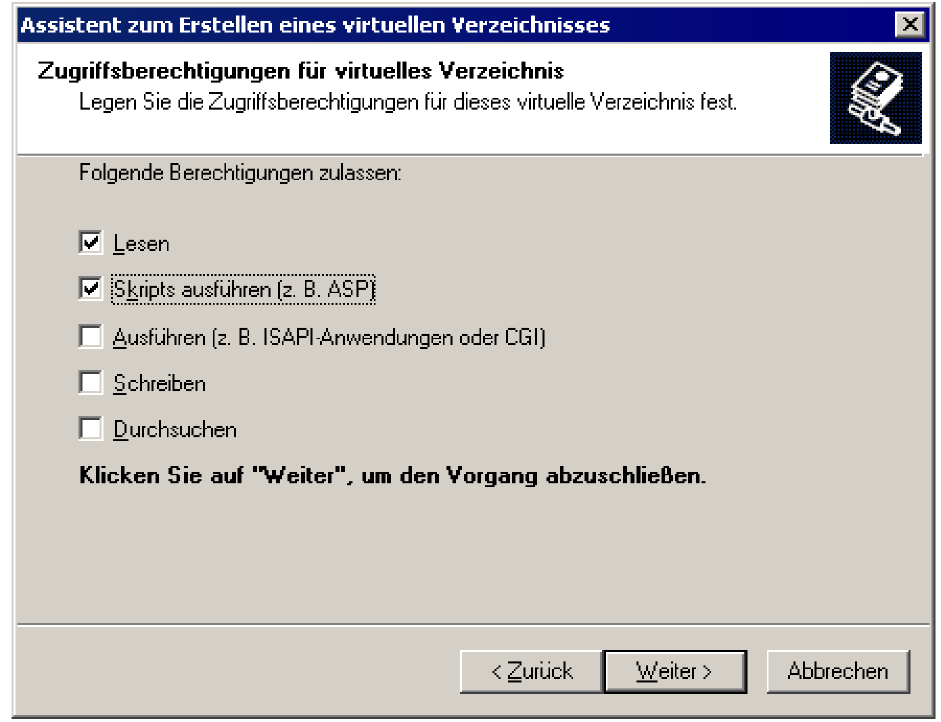


Bild 8 - Einstellung von Berechtigungen

4. Danach müssen Sie die Zugangsberechtigungen definieren. Markieren Sie die Kontrollkästchen für die **Read**- und **Run-Scripte (beispielsweise ASP)**. Kontrollieren Sie, ob alle anderen Kontrollkästchen deaktiviert sind. Klicken Sie auf **Weiter** und auf der Seite "Endbearbeitung" auf **Fertigstellen** um den Assistenten zum Erstellen des virtuellen Verzeichnisses zu beenden.

5. Klicken Sie mit der rechten Maustaste auf das neu erstellte virtuelle Verzeichnis unter dem Web-Hauptverzeichnis Ihres Website-Servers und wählen Sie aus dem Kontextmenü die Option **Eigenschaften**.

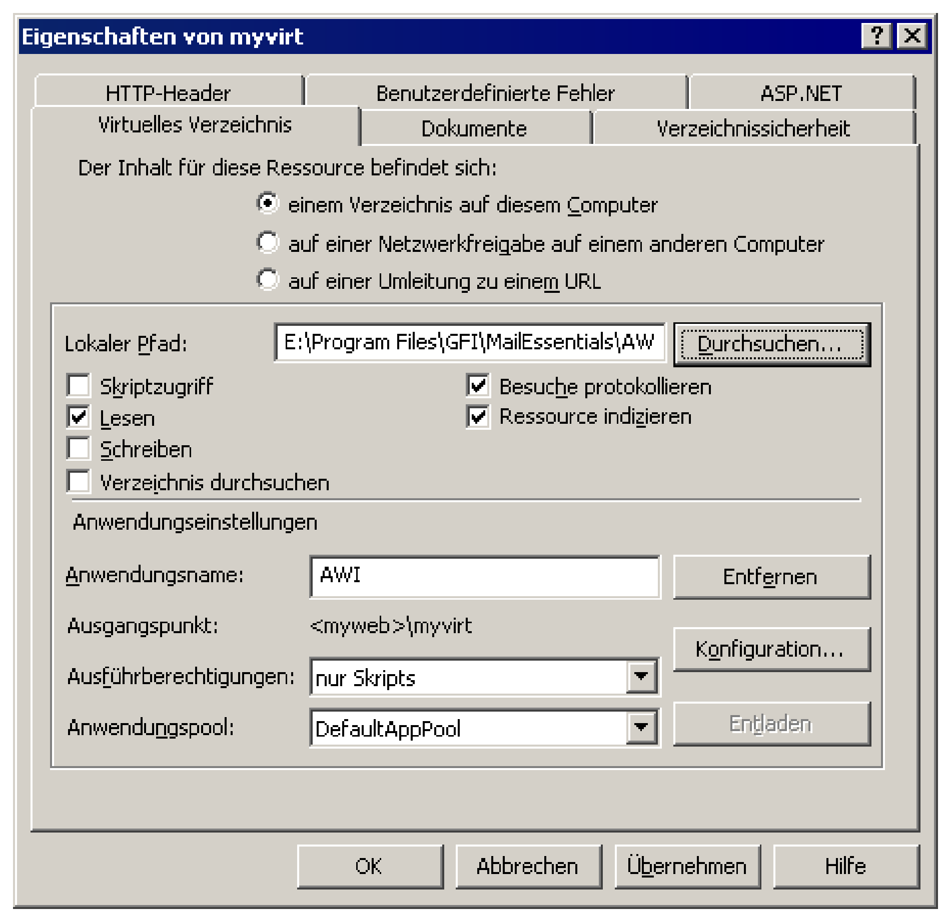


Bild 9 - Einstellung der Eigenschaften des virtuellen Verzeichnisses

6. Markieren Sie auf der Registerkarte **Virtuelles Verzeichnis** im Dialog **Eigenschaften** die Kontrollkästchen **Lesen**, **Besucher protokollieren** und **Diese Ressource indizieren**. Kontrollieren Sie, ob alle anderen Kontrollkästchen deaktiviert sind. Klicken Sie in dem Listenfeld **Berechtigungen ausführen** auf **Nur Skripte**.

7. Öffnen Sie die Registerkarte **Dokumente**. Entfernen Sie alle Standarddokumente außer **default.asp**.

8. Öffnen Sie die Registerkarte **Verzeichnissicherheit** und klicken Sie auf die Schaltfläche **Bearbeiten** in der **Authentifizierungs-** und **Zugriffskontrollgruppe**.

HINWEIS: Da das Archive Web Interface Zugriff auf alle E-Mails einräumt, die von GFI MailEssentials archiviert wurden, müssen Sie für diesen Webserver und das virtuelle Verzeichnis eine korrekte Authentifizierung und Sicherheit konfigurieren. Es gibt drei Möglichkeiten, die Suchschnittstelle zu sichern: Basisauthentifizierung-Bericht und integrierte Windows-Authentifizierung. Bei einer Umgebung mit Active Directory ist die integrierte Windows-Authentifizierung die bevorzugte Wahl, weil dann der Authentifizierungsprozess problemlos abläuft und die Benutzer weder nach Benutzernamen noch Kennwort gefragt werden. Stattdessen werden die aktuellen Windows-Benutzerinformationen auf dem Client-Computer zur Authentifizierung verwendet. Wenn Sie GFI MailEssentials in einer DMZ installieren, müssen Sie die Basisauthentifizierung verwenden.

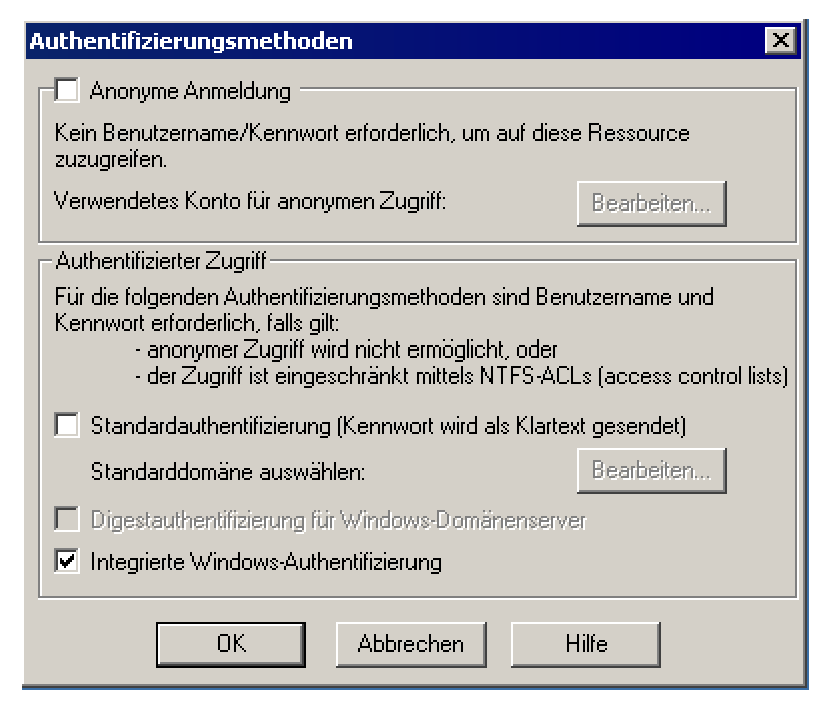


Bild 10 - Authentifizierungsverfahren auswählen

9. Markieren Sie das Kontrollkästchen **Integrierte Windows-Authentifizierung** (bei Installation im internen Netzwerk empfohlen) ODER das Kontrollkästchen **Basisauthentifizierung** (bei Installation in einer DMZ). Achten Sie darauf, dass das Kontrollkästchen **Anonymen Zugriff aktivieren** deaktiviert ist.

HINWEIS 1: Bei integrierter Windows-Authentifizierung erfolgt die Authentifizierung mit der Active Directory, das heißt, Sie müssen keine weiteren Benutzer konfigurieren. Wenn Sie die Basisauthentifizierung nutzen, erfolgt die Authentifizierung mit der lokalen Benutzerdatenbank auf dem Computer. Erstellen Sie in diesem Fall Benutzernamen und Kennwörter auf dem lokalen Computer. Weitere Informationen zur Sicherung von IIS finden Sie in der IIS-Dokumentation.

HINWEIS 2: **Achten Sie darauf, dass Sie KEINEN anonymen Zugriff einräumen.**

10. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Konfigurieren Sie die IIS Web-Anwendung für AWI auf ISS 7.0.

So konfigurieren Sie AWI für IIS 7.0:

1. Öffnen Sie die 'Administrator-Tools'.

2. Rufen Sie den 'Internet Information Services (IIS) Manager' auf.

3. Klicken Sie mit der rechten Maustaste auf die Website, die als Host für die AWI-Webschnittstelle dienen soll, und klicken Sie dann auf **Anwendung hinzufügen.**

4. Geben Sie 'AWI' als Alias ein und dann den Pfad zum Ordner 'AWI wwwroot' unter <GFI\MailEssentials\AWI\wwwroot>.

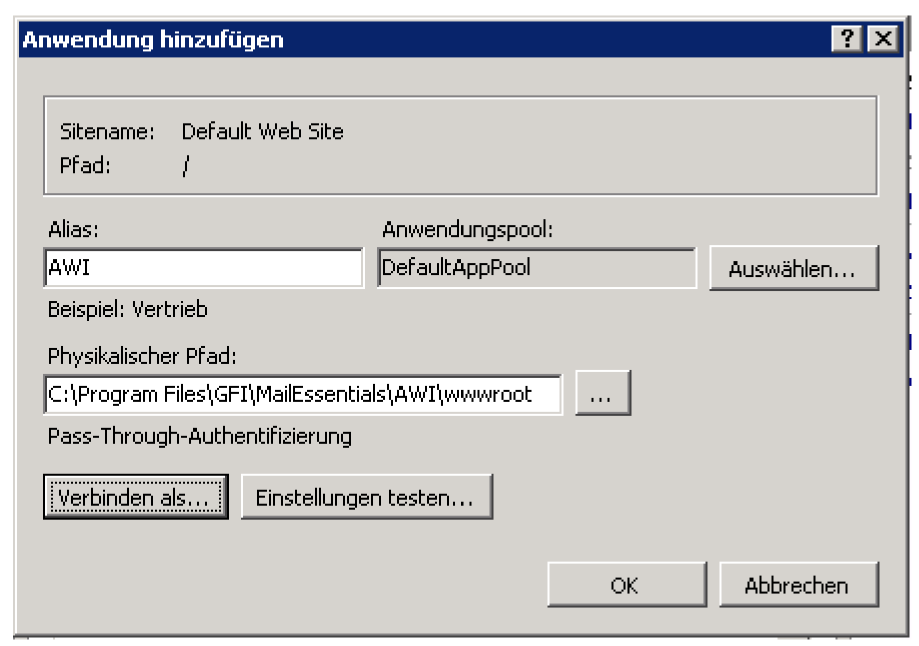


Bild 11 - Internet Information Services (IIS) Manager: Anwendung hinzufügen

5. Klicken Sie auf **OK** um die neue Anwendung zu erstellen.

6. Klicken Sie auf die gerade erstellte Anwendung 'AWI' und doppelklicken Sie auf das Symbol **Authentifizierung** auf der rechten Seite.

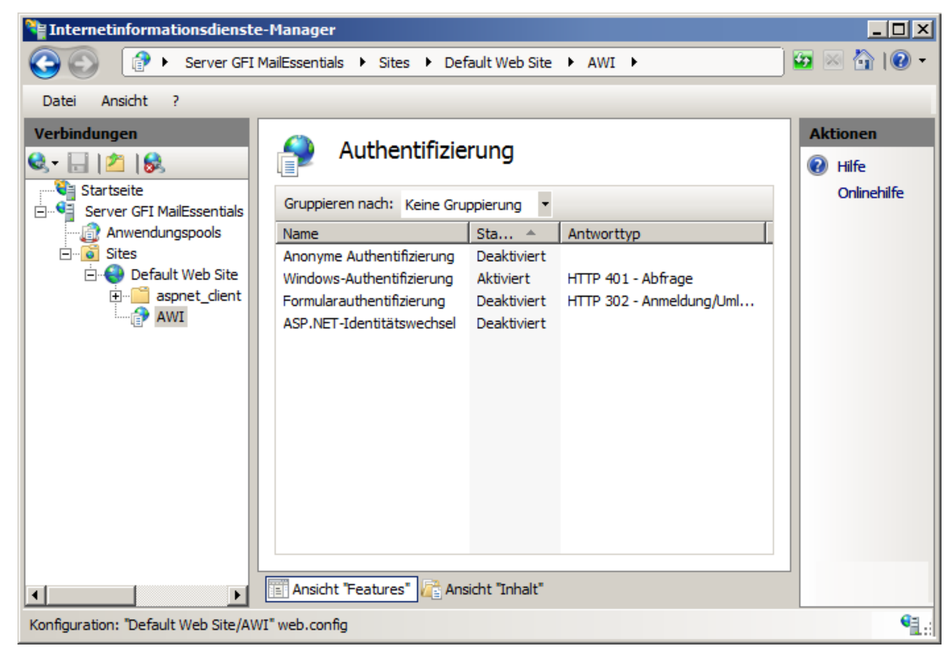


Bild 12 - Internet Information Services (IIS) Manager

7. Klicken Sie mit der rechten Maustaste auf die Option **Anonyme Authentifizierung** und dann auf **Deaktivieren**.

8. Klicken Sie mit der rechten Maustaste auf die Option **Windows Authentifizierung** und dann auf **Aktivieren**.

3.6.3 Zugriff auf das Archive Web Interface

1. Starten Sie Internet Explorer.

2. Geben Sie Folgendes ein: *http://<computer_name>/<awi_virtueller_ordner_name>*.

- **Beispiel:** http://master-domain.com/awi/

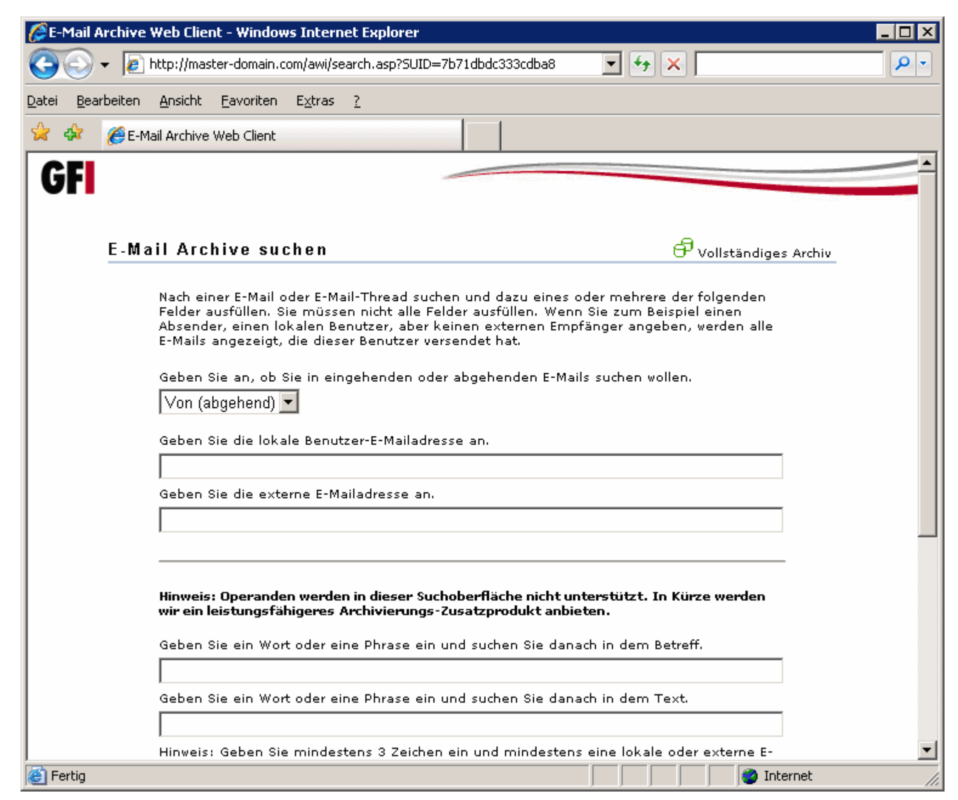


Bild 13 - Die Suchseite Archive Web Interface (AWI)

AWI lädt die Suchseite. Klicken Sie auf den Link **Gesamtes Archiv** in der oberen rechten Ecke um die Seite für das Gesamtarchiv aufzurufen.

3.7 Berichte zur E-Mail-Verarbeitung und zum Spam-Status

GFI MailEssentials erlaubt die Erstellung von Berichten über in der Datenbank archivierte Daten. Mit Hilfe dieser Berichte erkennen Sie, welche Spam-Mails von GFI MailEssentials ausgefiltert werden und wie Ihre Domänenressourcen und Ihr Mailserver ausgelastet sind.

Wichtige Hinweise

Aktivieren Sie die Archivierung von GFI MailEssentials um die Berichtfunktionen zu nutzen. Details zur Aktivierung der Archivierungsfunktion finden Sie im Abschnitt Aktivieren der Archivierung auf Seite 21 dieses Handbuchs.

3.7.1 Aktivieren von Berichten

1. Klicken Sie auf **E-Mail-Verwaltung ► Berichterstellung ► Eigenschaften** und anschließend auf die Schaltfläche **Konfigurieren**.

2. Wählen Sie dann den Datenbanktyp aus:

- **Microsoft Access** - Geben Sie Dateiname und Standort an.

- **Microsoft SQL Server** - Geben Sie Servername, Authentifizierungsdaten und Datenbank an.

3. Klicken Sie auf die Schaltfläche **Testen** um die Datenbankkonfiguration zu testen. Klicken Sie auf **OK** um die Einstellung zu speichern.

3.7.2 Verwendung von Berichten

1. Starten Sie die Berichterstattung von GFI MailEssentials, indem Sie auf **Start ► Alle Programme ► GFI MailEssentials ► GFI MailEssentials-Berichte** klicken.

2. Klicken Sie auf die Option **Berichte** und wählen Sie dann einen Bericht /eine Statistik auf der Seite Statistik aus.

3. Klicken Sie auf die Menüoption **Datei ► Drucken** um Berichte auszudrucken.

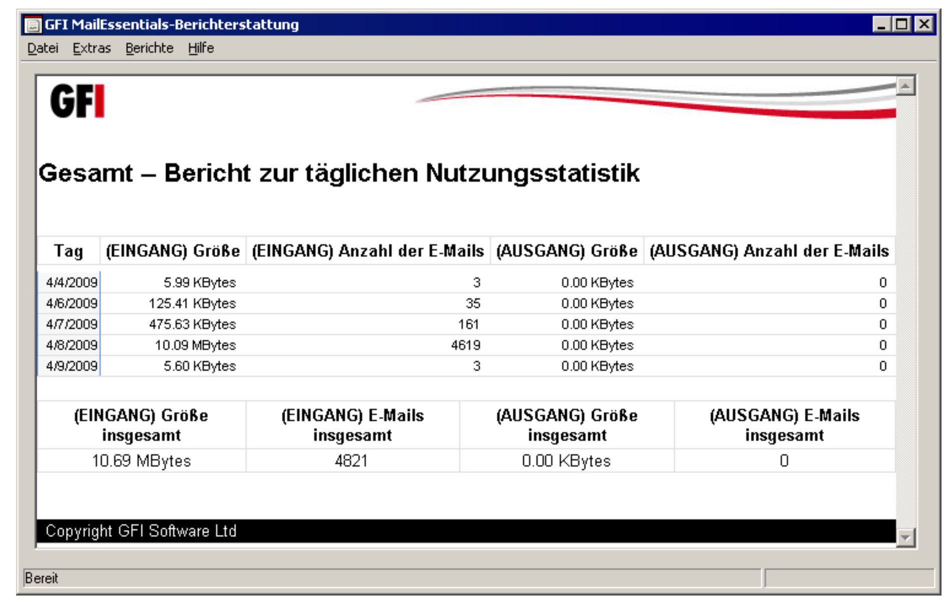
HINWEIS: Klicken Sie auf **Datei ► Drucken Vorschau** um eine Druckvorschau anzuzeigen.

4. Zum Speichern eines Berichts klicken Sie auf **Datei ► Speichern unter**. Geben Sie Name und Speicherort für die gespeicherte Datei ein und klicken Sie auf die Schaltfläche **Speichern**.

HINWEIS: Der Bericht wird an dem ausgewählten Ort mit dem angegebenen Dateinamen gespeichert. In dem angegebenen Ordner werden zwei Unterordner erstellt, 'graphics' und 'report'. Der Unterordner 'report' enthält die Berichtdateien im HTML-Format. Der Unterordner 'graphics' enthält die Grafiken, die in dem HTML-Bericht enthalten sind.

Täglicher Spam-Bericht

Der tägliche Spam-Bericht zeigt die Gesamtzahl der verarbeiteten E-Mails, die Gesamtzahl der erkannten Spam-Mails, den prozentualen Anteil der Spam-Mails an allen Mails und wie viele Spam-Mails durch jedes einzelne Spam-Funktion erkannt wurden. Jede Zeile in dem Bericht entspricht einem Tag.



Gesamt – Bericht zur täglichen Nutzungsstatistik

Tag	(EINGANG) Größe	(EINGANG) Anzahl der E-Mails	(AUSGANG) Größe	(AUSGANG) Anzahl der E-Mails
4/4/2009	5.99 KBytes	3	0.00 KBytes	0
4/6/2009	125.41 KBytes	35	0.00 KBytes	0
4/7/2009	475.63 KBytes	161	0.00 KBytes	0
4/8/2009	10.09 MBytes	4619	0.00 KBytes	0
4/9/2009	5.60 KBytes	3	0.00 KBytes	0

(EINGANG) Größe insgesamt	(EINGANG) E-Mails insgesamt	(AUSGANG) Größe insgesamt	(AUSGANG) E-Mails insgesamt
10.69 MBytes	4821	0.00 KBytes	0

Copyright GFI Software Ltd

Bild 14 - Täglicher Spam-Bericht

Berichtsoptionen

- **Spalte sortieren:** Sortieren Sie den Bericht nach Datum, Gesamtzahl der verarbeiteten Spams, Keyword-Prüfung usw.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Tage pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich:** Beschränken Sie den Bericht auf einen bestimmten Datumsbereich.

Wenn Sie alle Berichtoptionen ausgewählt haben, klicken Sie auf **Bericht** um den Bericht zu erzeugen.

Anti-Spam-Regeln-Bericht

Der Bericht mit den Anti-Spam-Regeln zeigt, wie viele Spam-Mails mit jedem Spam-Filter erkannt wurden.

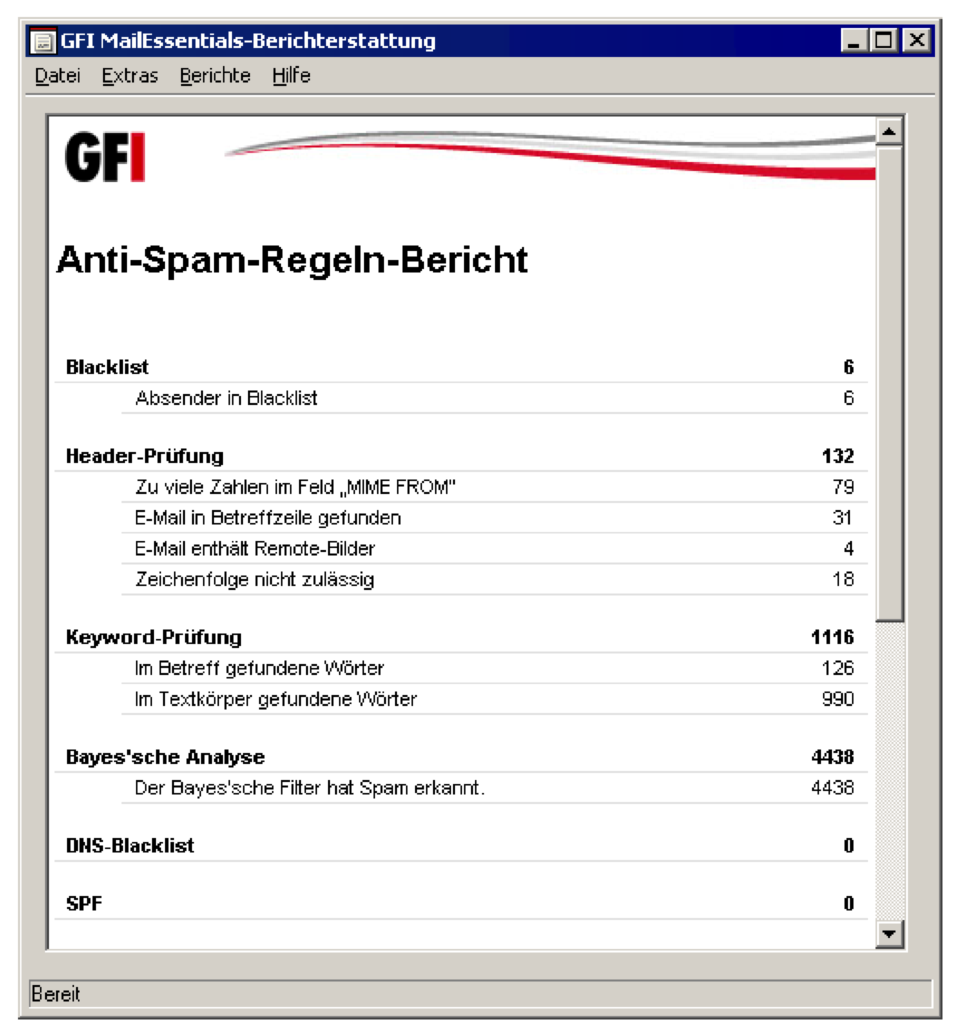


Bild 15 - Anti-Spam-Regeln-Bericht

Berichtsoptionen

- **Spezifische E-Mail:** Beschränkt den Bericht auf eine bestimmte E-Mail-Adresse.

- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Benutzer-Nutzungsstatistiken

Der Bericht mit den Benutzer-Nutzungsstatistiken zeigt in einer Übersicht, wie viele E-Mails die Benutzer versenden oder empfangen und wie groß die versendeten oder empfangenen E-Mails sind.

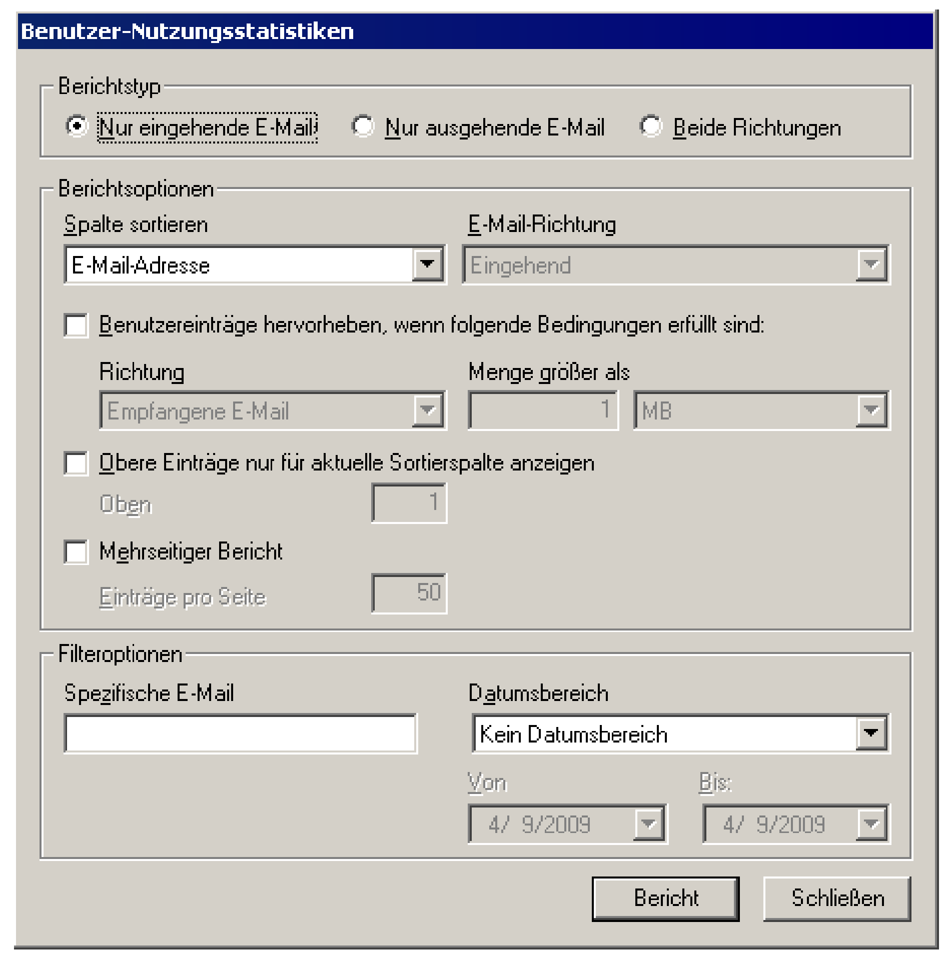


Bild 16 - Filterdialog "Benutzer-Nutzungsstatistik"

Berichtstyp

- **Berichtstyp:** Geben Sie an, ob Sie einen Bericht für die eingehenden E-Mails, die ausgehenden E-Mails oder beide erstellen wollen.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob die Sortierung nach E-Mail-Adresse, nach Anzahl der E-Mails oder nach der Gesamtgröße der E-Mails erfolgen soll.
- **Benutzer hervorheben:** Identifizieren Sie die Benutzer, die ungewöhnlich viele E-Mails oder ungewöhnlich große E-Mails empfangen oder versenden.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten Benutzer

in dem Bericht an.

- **Mehrseitiger Bericht:** Geben Sie an, wie viele Benutzer pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich**: Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Domänen-Nutzungsstatistiken

Die Bericht mit der Domänen-Nutzungsstatistik zeigt in einer Übersicht, wie viele E-Mails an externe Domänen gesendet oder von dort empfangen wurden.

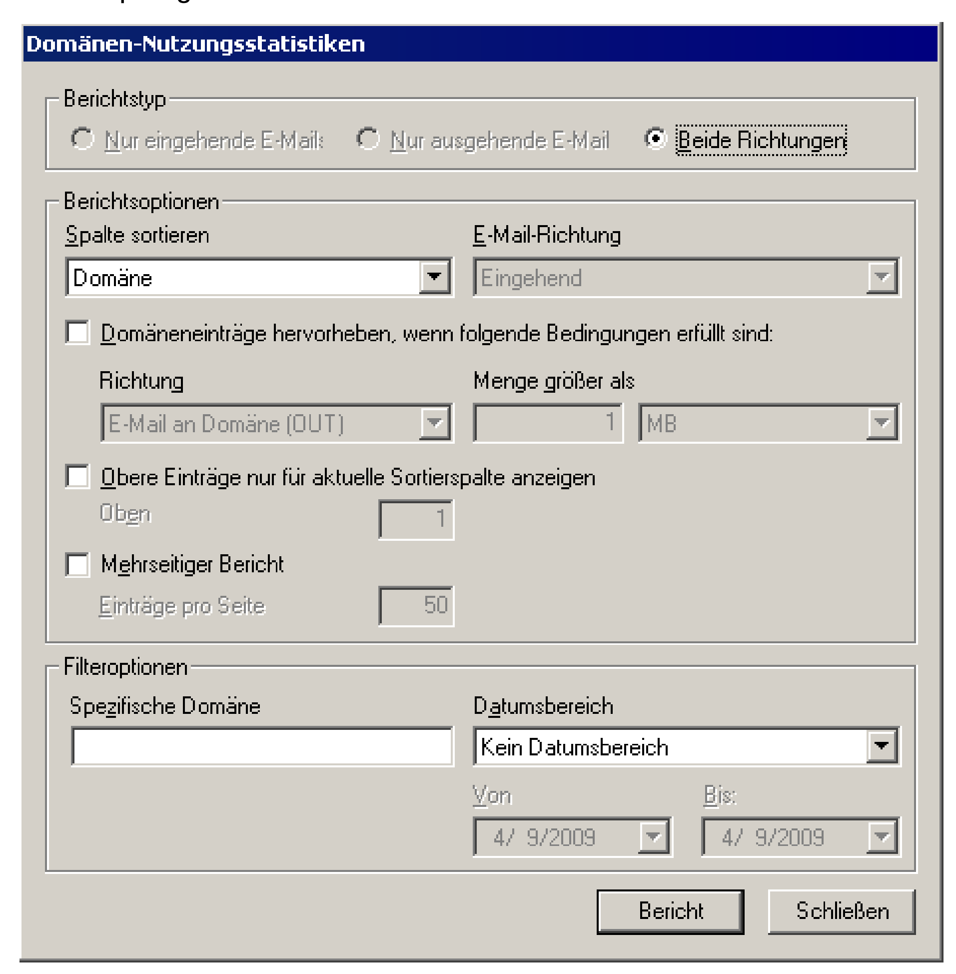


Bild 17 - Der Filterdialog "Domänen-Nutzungsstatistik"

Berichtstyp

- **Berichtstyp:** Standardmäßig enthält die Domänen-Nutzungsstatistik immer Daten für ausgehende und eingehende E-Mails.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob der Bericht nach

Domänenname, nach Anzahl der E-Mails oder nach Gesamtgröße der E-Mails sortiert werden soll.

- **Domänen hervorheben:** Geben Sie die Domänen an, die eine ungewöhnlich große Zahl E-Mails oder ungewöhnlich große E-Mails empfangen oder versenden.
- **Nur wichtige anzeigen:** Zeigt nur die wichtigsten Domänen in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Domänen pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische Domäne:** Beschränkt den Bericht auf eine bestimmte Domäne.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Tägliche E-Mail-Server-Nutzungsstatistiken

Dieser Bericht zeigt in einer Übersicht, wie viele E-Mails pro Tag von dem E-Mail-Server empfangen oder versendet werden, auf dem GFI MailEssentials installiert ist.

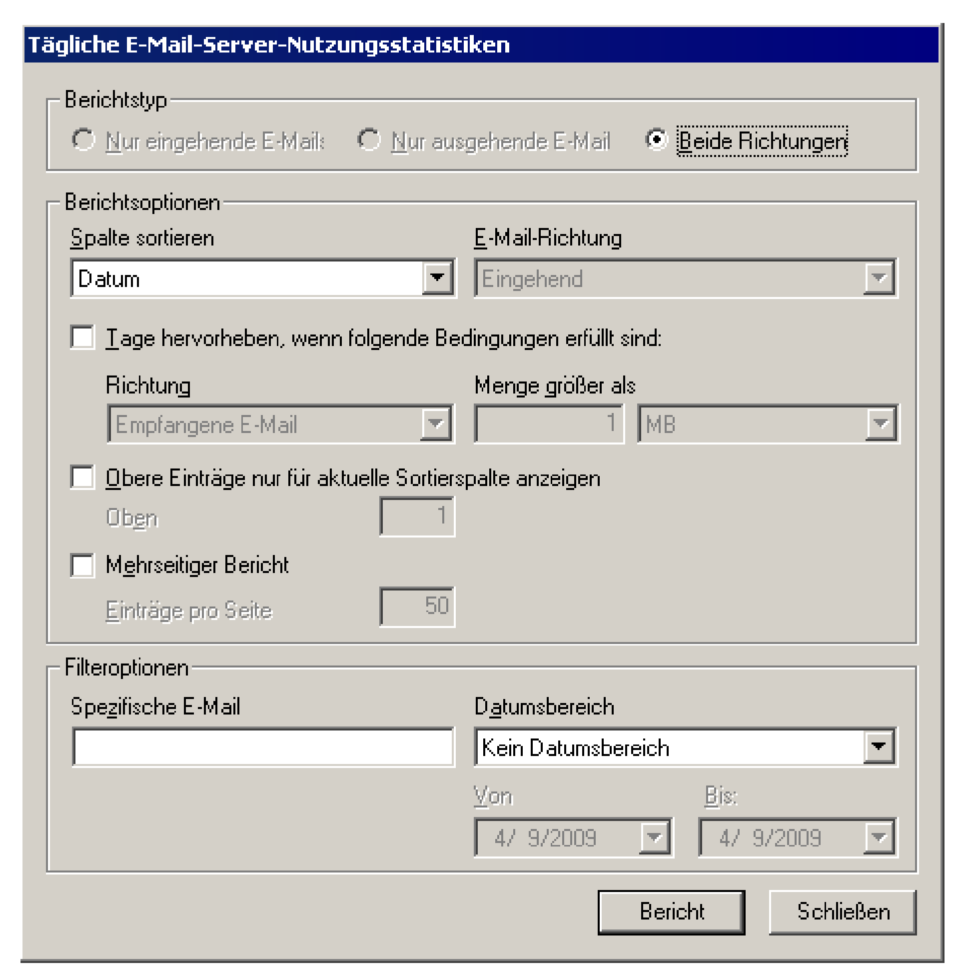


Bild 18 - Filterdialog "Tägliche E-Mail-Server-Nutzungsstatistik"

Berichtstyp

- **Berichtstyp:** Die Daten für die tägliche E-Mail-Server-Nutzungsstatistik werden immer für eingehende und ausgehende E-Mails angezeigt.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob der Bericht nach Datum sortiert werden soll (da der Bericht täglich erstellt wird), nach der Anzahl der E-Mails oder nach der Gesamtgröße der E-Mails.
- **Tage hervorheben:** Geben Sie die Tage an, an denen Sie mehr E-Mails oder größere E-Mails empfangen oder versendet haben als vordefiniert.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten definierten Tage in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Tage pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränkt den Bericht auf eine bestimmte Domäne.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Benutzerkommunikation

Der Bericht Benutzerkommunikation erlaubt Ihnen, zu kontrollieren, welche Art von E-Mails jeder Benutzer versendet hat. Wenn der Bericht zur Benutzerkommunikation einmal erstellt ist, kann der Benutzereintrag erweitert werden um den Betreff der gesendeten oder empfangenen E-Mails anzuzeigen. E-Mails mit dem gleichen Betreff werden in Gruppen zusammengefasst. Diese E-Mails können dann weiter analysiert werden um zu prüfen, wann und an wen die E-Mail mit dem Betreff gesendet wurde.

Wichtige Hinweise

1. Dieser Bericht ist ein komplexer Bericht und seine Erstellung benötigt Zeit. Sie sollten den Umfang des Berichts auf einen bestimmten Benutzer oder einen bestimmten Datumsbereich einschränken.

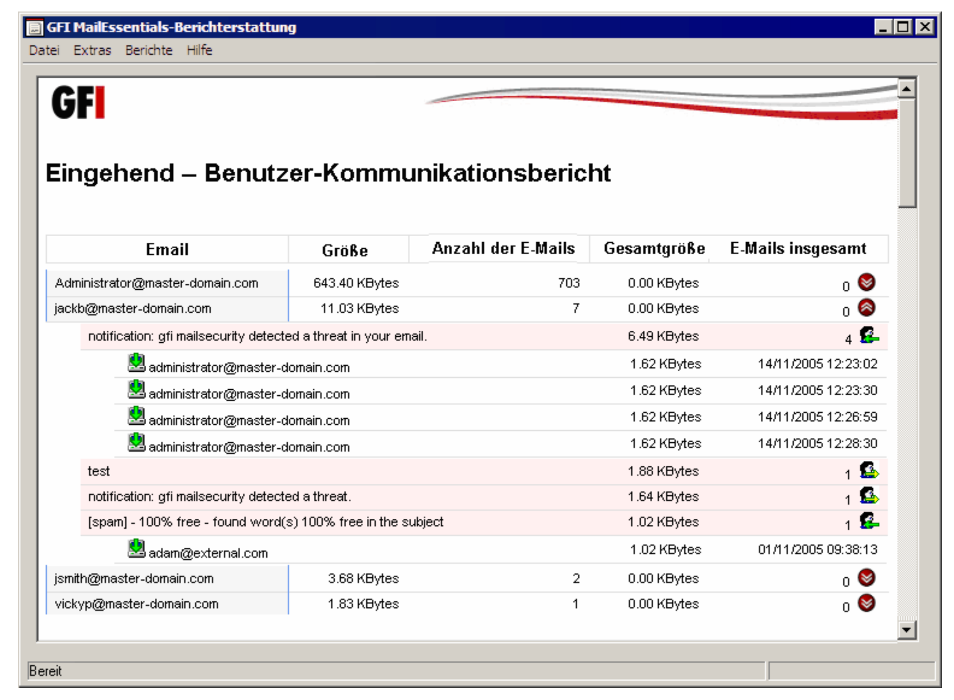


Bild 19 - Der Bericht Benutzerkommunikation zeigt eine genaue E-Mail-Analyse.

Berichtstyp

- **Berichtstyp:** Geben Sie an, ob Sie einen Bericht für die eingehenden E-Mails, die ausgehenden E-Mails oder beide erstellen wollen.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob der Bericht nach E-Mail-Adresse, nach Anzahl der E-Mails oder nach Gesamtgröße der E-Mails sortiert werden sollte.
- **Benutzer hervorheben:** Identifizieren Sie Benutzer, die ungewöhnlich viele oder ungewöhnlich große E-Mails empfangen oder versendet haben.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten Benutzer in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Benutzer pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Klicken Sie bei Auswahl der betreffenden Optionen auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

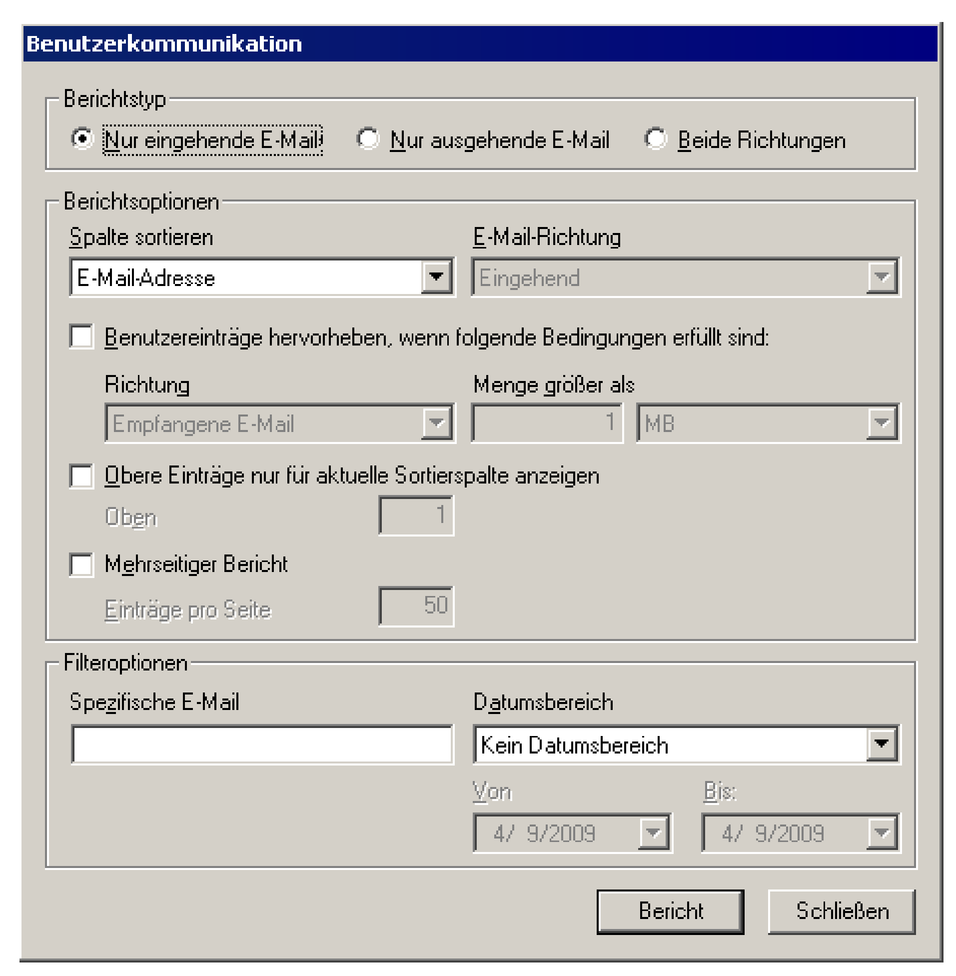


Bild 20 - Filterdialog "Benutzer-Kommunikation"

Sonstige Optionen

- **Ausschluss von Benutzern aus Berichten**

  Mit dem Tool zum Ausschluss von Benutzern können Benutzer aus Berichten ausgeblendet werden.

  Klicken Sie auf **Tools ► Benutzerausschlussliste** und dann auf die Schaltfläche **Hinzufügen**, damit Sie die SMTP-E-Mail-Adresse für den Benutzer, der bei Berichten ignoriert werden soll, **hinzufügen** oder **entfernen** können.

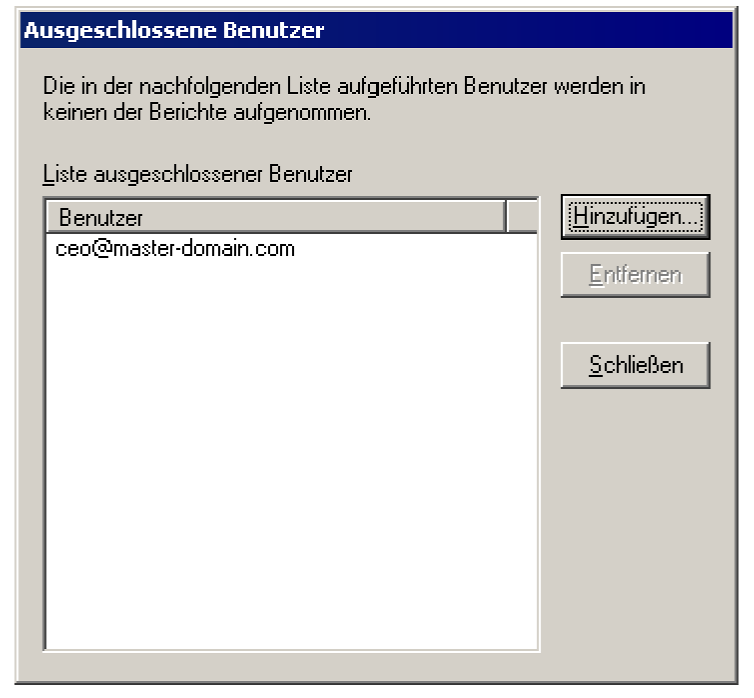


Bild 21 - Der Dialog "Ausgeschlossene Benutzer"

Such-Tool

Mit dem Such-Tool können Sie Text-Strings in Berichten finden.

Geben Sie in der Menüoption **Tools ► Suchen** die Text-Strings ein, die gefunden werden sollen, und klicken Sie dann zur Suche auf **Nächsten suchen**.

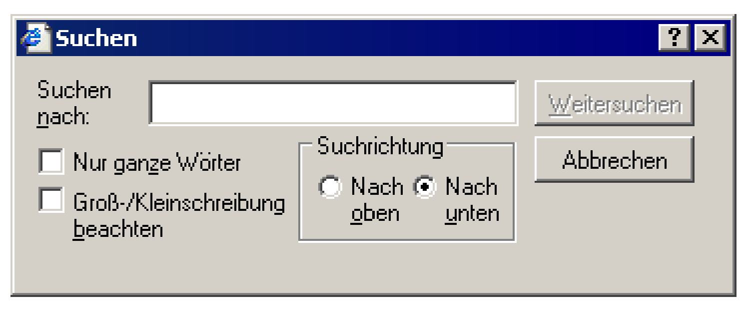


Bild 22 - Der Dialog "Suchen"

3.8 Deaktivieren/Aktivieren des E-Mail-Verarbeitung

Mit Deaktivierung des Scannens deaktivieren Sie alle Schutzfunktionen von GFI MailEssentials, sodass alle E-Mails, auch Spam-Mails, in die Benutzerpostfächer gelangen.

So aktivieren/deaktivieren Sie das Scannen von E-Mails mit GFI MailEssentials:

1. Klicken Sie auf **Start ► Programme ► GFI MailEssentials ► GFI MailEssentials Switchboard**.

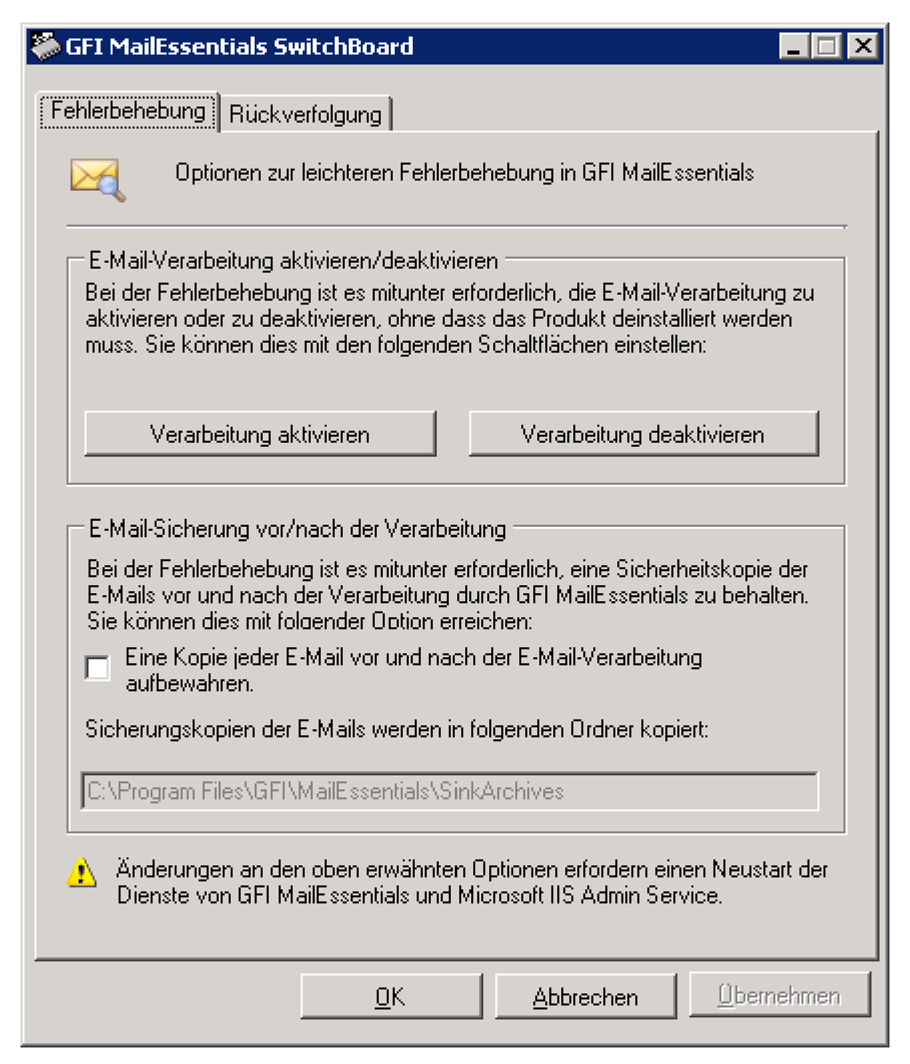


Bild 23 - Im GFI MailEssentials Switchboard: Fehlerbehebung

2. Klicken Sie auf die Registerkarte **Fehlerbehebung**:

- und dann auf **Verarbeitung deaktivieren**, um das Scannen von E-Mails zu deaktivieren.
- und dann auf **Verarbeitung aktivieren**, um das Scannen von E-Mails zu aktivieren.

Der Scan von E-Mails kann durch einen Befehl in der Befehlszeile aktiviert und deaktiviert werden. Weitere Informationen finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003468.

4 Kundenspezifische Anpassung von GFI MailEssentials

4.1 Ergänzung zusätzlicher Domänen eingehender E-Mails

Anhand der Domänen eingehender E-Mails kann GFI MailEssentials zwischen eingehenden und ausgehenden E-Mails unterscheiden und somit die E-Mails identifizieren, die auf Spam untersucht werden sollten. Bei der Installation werden die Domänen der eingehenden E-Mails über den Dienst IIS SMTP importiert.

In einigen Fällen kann jedoch eine lokale E-Mail-Umleitung in IIS eine abweichende Konfiguration erfordern:

Beispiel: Dies trifft zu für Domänen, die für E-Mail-Umleitung lokal sind, für Ihren Mail-Server jedoch nicht.

Die Anweisungen in diesem Abschnitt erläutern, wie Sie nach der Installation Domänen eingehender E-Mails ergänzen oder entfernen.

Wichtige Hinweise

1. Jede Domäne, über die Sie E-Mails empfangen und die nicht in der Konfiguration für Domänen eingehender E-Mails aufgeführt ist, ist nicht durch GFI MailEssentials vor Spam geschützt.

4.1.1 Hinzufügen und Entfernen von Inbound-Domänen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Allgemein ► Allgemein Einstellungen**, dann auf **Eigenschaften** und auf die Registerkarte **Lokale Domänen**.

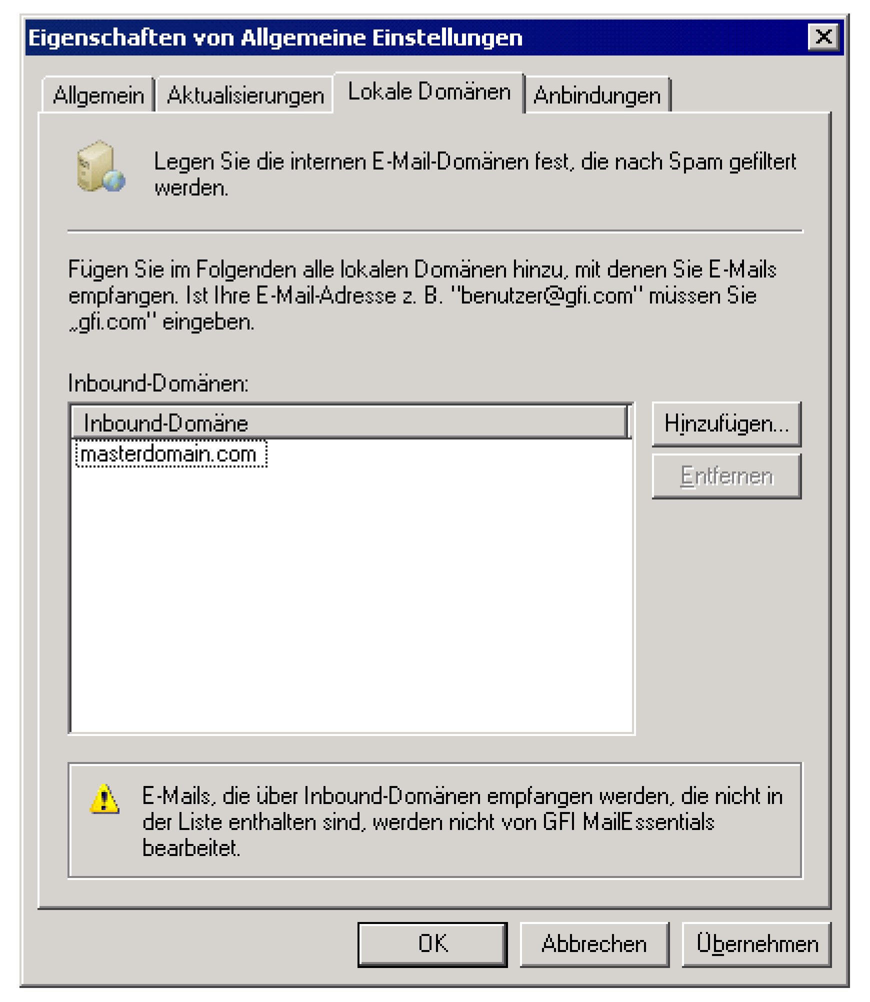


Bild 24 - Hinzufügen einer Domäne für eingehende E-Mails

2. Klicken Sie auf die Schaltfläche **Hinzufügen…** und geben Sie die Details der Domäne ein, die Sie als neue Domäne für eingehende E-Mails hinzufügen wollen. Wählen Sie zum Entfernen von Domänen die betreffende Domäne aus und klicken Sie auf **Entfernen**.

3. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

4.2 Spam-Filter

GFI MailEssentials nutzt verschiedene Spam-Filter zur Identifizierung von Spam:

Filter	Beschreibung	Standard-mäßig aktiviert
SpamRazer	Ein Spam-Filter, der erkennt, ob eine E-Mail Spam ist. Dazu wird die E-Mail-Herkunft, der Inhalt der Nachricht und deren Transportweg analysiert.	Ja
Directory Harvesting	Das Modul stoppt E-Mails, die nach dem Zufallsprinzip erzeugt an einen Server gesendet werden, für die aber meist keine Benutzer existieren.	Ja
Phishing	Dieser Filter blockiert E-Mails, die Links in den Nachrichtentexten enthalten, die auf bekannte Phishing-Sites zeigen oder typische Phishing-Keywords enthalten.	Ja

Sender Policy Framework	Dieser Filter stoppt E-Mails, die von Domänen stammen, die in den SPF-Records nicht autorisiert wurden.	Nein
Auto-Whitelist	Wenn an diese Adressen eine E-Mail gesendet wird, werden Spam-Filter automatisch ignoriert.	Ja
Whitelists	Eine benutzerdefinierte Liste sicherer E-Mail-Adressen	Ja
Email Blacklist	Eine benutzerdefinierte Liste gesperrter E-Mail-Nutzer oder Domänen.	Ja
DNS-Blacklists	Prüft, ob die empfangene E-Mail von Absendern stammt, die in einer öffentlichen DNS-Blacklist bekannter Spammer enthalten sind.	Ja
Spam URI Realtime Blocklists	Dieser Filter stoppt E-Mails, die Links zu Domänen enthalten, die in den öffentlichen Spam-URL-Blocklists enthalten sind, beispielsweise sc.surbl.org.	Ja
Header-Prufüng	Dieses Modul analysiert die einzelnen Felder im Header durch Vergleich mit dem SMTP- und MIME-Feld.	Ja
Keyword-Prufüng	Spam-Mails werden anhand gesperrter Keywords in der E-Mail-Überschrift oder in der E-Mail-Nachricht identifiziert.	Nein
Neue Absender	E-Mails, die von Absendern stammen, an die noch nie eine E-Mail gesendet wurde.	Nein
Bayes'sche Analyse	Ein Anti-Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.	Nein

4.2.1 Spam-Aktionen

GFI MailEssentials kann, wenn eine Nachricht als Spam identifiziert wurde, verschiedene Aktionen ausführen. Dies sind:

- Löschen der Nachricht
- Verschieben der Nachricht in einen zentralen Ordner
- Weiterleitung der Nachricht an eine E-Mail-Adresse
- Kennzeichnung (Tagging) der Nachricht
- Verschieben der Nachricht in einen Junk-Ordner.

HINWEIS: Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

4.2.2 SpamRazer

SpamRazer ist der wichtigste Spam-Filter von GFI und standardmäßig nach der Installation aktiviert. Für SpamRazer werden häufige Aktualisierungen angeboten um schnell auf neue Spam-Trends zu reagieren.

HINWEIS: SpamRazer ist außerdem auch der Spam-Filter, der NDR-Spam blockiert. Weitere Informationen über GFI MailEssentials und NDR-Spam finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003322

Konfiguration von SpamRazer

HINWEIS 1: Eine Deaktivierung von SpamRazer wird NICHT empfohlen.

HINWEIS 2: GFI MailEssentials lädt SpamRazer-Aktualisierungen von folgender Adresse herunter: http://sn92.mailshell.net

1. Wählen Sie **Anti-Spam** ► **Anti-Spam-Filter** ► **SpamRazer** ► **Eigenschaften**.

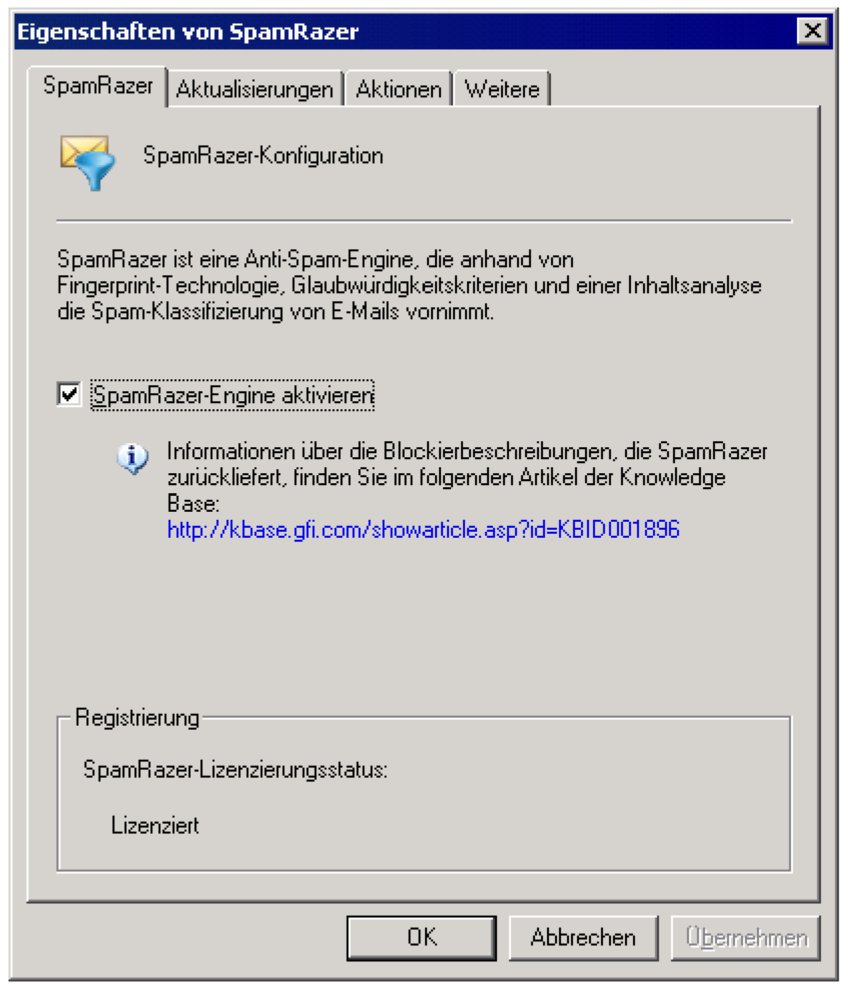


Bild 25 - SpamRazer-Eigenschaften

2. Führen Sie auf der Registerkarte **SpamRazer** eine der folgenden Aktionen aus:

- Aktivieren/deaktivieren Sie das Kontrollkästchen **SpamRazer aktivieren** um SpamRazer zu aktivieren oder zu deaktivieren.

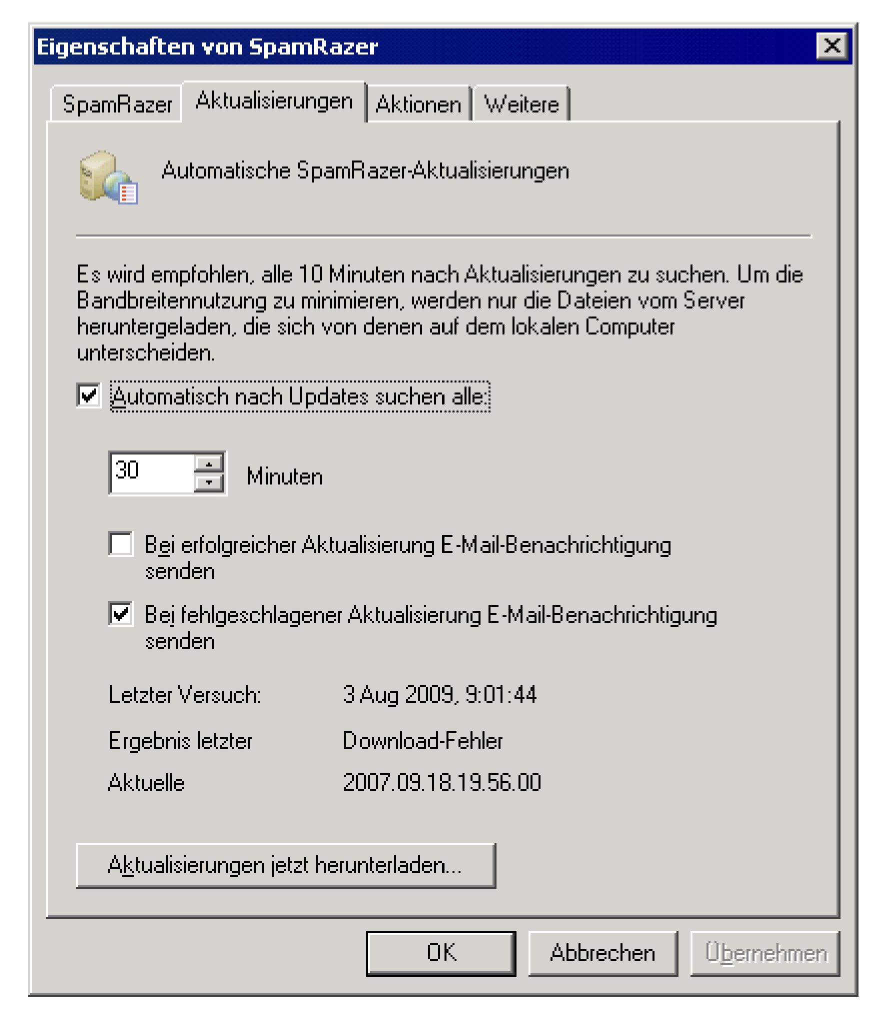


Bild 26 - Automatische SpamRazer-Aktualisierungen

3. Führen Sie auf der Registerkarte **Aktualisierungen** eine der folgenden Aktionen aus:

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Automatisch nach Updates suchen** um GFI MailEssentials so zu konfigurieren, dass das Programm automatisch SpamRazer-Updates sucht und diese herunterlädt. Geben Sie das Zeitintervall für die Prüfung auf Updates in Minuten an.

  HINWEIS: Wir empfehlen, diese Option für SpamRazer aktiviert zu lassen, damit die aktuellsten Spam-Trends effektiver erkannt werden.

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden, wenn ein Update erfolgreich war**, damit Sie per E-Mail informiert werden, ob neue Updates heruntergeladen sind.
- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden wenn das Update fehlschlägt**, damit Sie informiert werden, wenn ein Download oder eine Installation fehlgeschlagen ist.
- Klicken Sie auf **Updates jetzt herunterladen ...** um die Updates herunterzuladen.

HINWEIS: Hinweise zum Herunterladen von Updates über einen Proxyserver finden Sie unter Konfigurieren automatischer Updates auf Seite 120 in diesem Handbuch.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.3 Phishing

Phishing ist ein E-Mail-Verfahren, das die E-Mail-Benutzer bewegen soll, Spammern persönliche Daten preiszugeben. Eine Phishing-E-Mail ist meist so gestaltet, dass sie einer offiziellen E-Mail von einer vertrauenswürdigen Stelle, beispielsweise einer Bank, ähnelt. Phishing-E-Mails enthalten in der Regel Anweisungen, dass Benutzer sensitive Informationen, beispielsweise Online-Banking-Zugangsdaten oder Kreditkartendaten, bestätigen sollen. Phishing-E-Mails enthalten in der Regel einen Phishing Uniform Ressource Identifier (URI), den der Leser aufrufen soll um bestimmte sensitive Informationen auf einer Phishing-Site einzugeben. Diese Seite, auf die die Phishing-URI zeigt, kann eine Kopie einer offiziellen Website sein, wird jedoch von demjenigen kontrolliert, der die Phishing-E-Mails versendet hat. Wenn der Benutzer sensitive Daten auf der Phishing-Website eingibt, werden die Daten gesammelt und beispielsweise genutzt um Geld von Bankkonten abzuheben.

Die Funktion Phishing erkennt Phishing-E-Mails, da sie die in der E-Mail erhaltene URI mit einer Datenbank bekannter URIs vergleicht, die für Phishing-Angriffe verwendet wurden. Die Funktion Phishing sucht außerdem in den URIs nach typischen Phishing-Keywords.

Der Phishing-Filter ist standardmäßig nach der Installation aktiviert.

Konfiguration des Phishing

HINWEIS 1: Eine Deaktivierung des Phishing wird NICHT empfohlen.

1. Wählen Sie **Anti-Spam ► Anti-Spam-Filter ► Phishing ► Eigenschaften**.

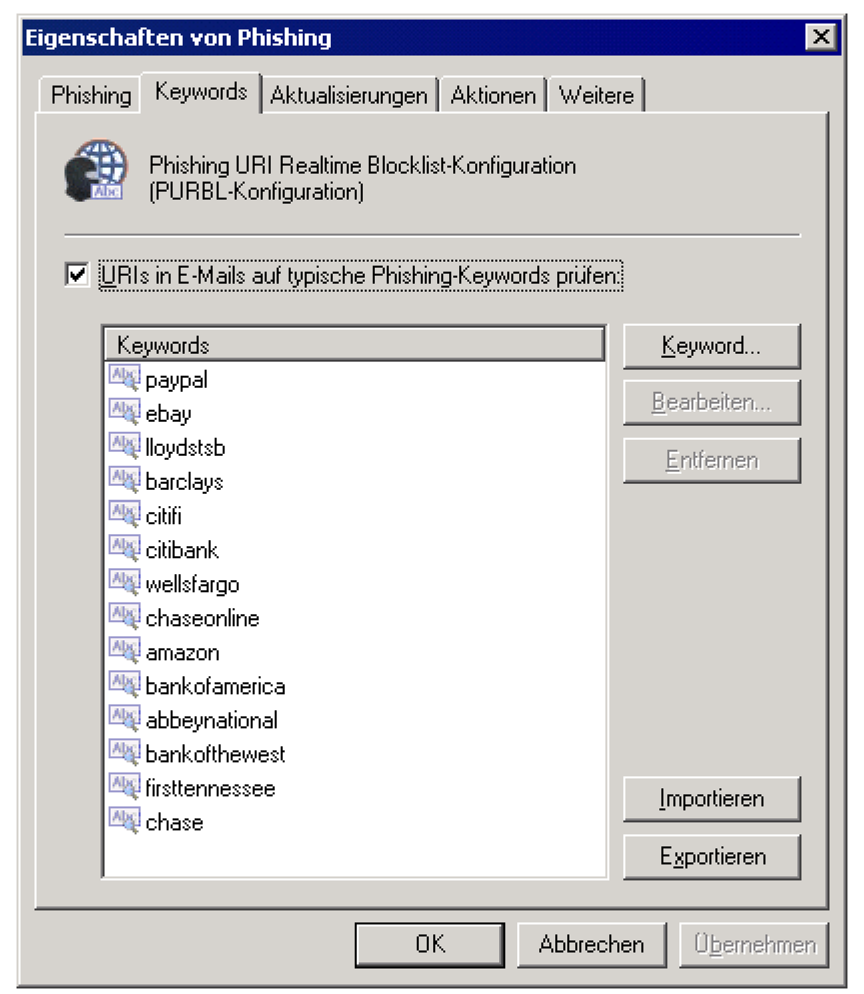


Bild 27 - Phishing-Keywords

2. Klicken Sie auf der Registerkarte **Phishing** auf folgende Aktionen:

- Aktivieren/deaktivieren Sie die Option **E-Mails auf URIs bekannter Phishing-Websites prüfen** um PURBL zu aktivieren oder zu deaktivieren.

3. Führen Sie auf der Registerkarte **Keywords** folgende Aktionen aus:

- Aktivieren oder deaktivieren Sie die Option **URIs in E-Mails auf typische Phishing-Keywords prüfen** um typische Phishing-Keywords zu aktivieren oder zu deaktivieren.
- Klicken Sie auf die Schaltfläche **Keyword** und geben Sie die Keywords in dem Dialog **Keyword eingeben** ein um Keywords in dem PURBL-Filter zu ergänzen.
- Wählen Sie ein Keyword aus und klicken Sie auf **Bearbeiten** oder **Entfernen** um das eingegebene Keyword zu bearbeiten oder aus dem Phishing-Filter zu entfernen.
- Klicken Sie auf **Exportieren** um die aktuelle Keyword-Liste im XML-Format zu exportieren.
- Klicken Sie auf **Importieren** um die zuvor in XML exportierte Keyword-Liste wieder zu importieren.

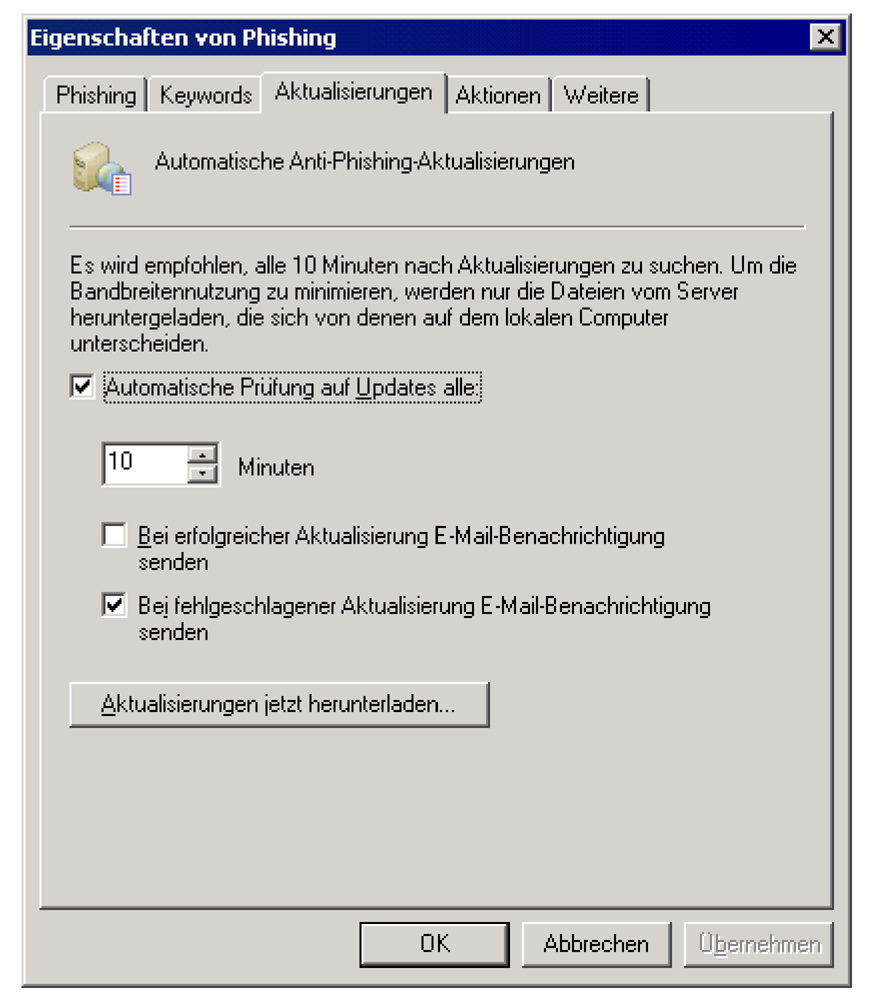


Bild 28 - Automatische Anti-Phishing-Aktualisierungen

4. Führen Sie auf der Registerkarte **Aktualisierungen** eine der folgenden Aktionen aus:

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Automatisch auf Aktualisierungen prüfen** um die automatische Prüfung und das Herunterladen von Anti-Phishing-Aktualisierungen zu aktivieren bzw. zu deaktivieren.

  HINWEIS: Wir empfehlen, unbedingt diese Option zu aktivieren, da durch häufige Aktualisierungen Phishing die jüngsten Phishing-E-Mails effektiver erkannt werden.

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden, wenn eine Aktualisierung erfolgreich war**, damit Sie per E-Mail informiert werden, ob neue Aktualisierungen heruntergeladen sind.

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden wenn die Aktualisierung fehlschlägt**, damit Sie informiert werden, wenn ein Download oder eine Installation fehlgeschlagen ist.

HINWEIS: Hinweise zum Herunterladen von Updates über einen Proxyserver finden Sie unter Konfigurieren automatischer Updates Auf Seite 120 in diesem Handbuch

5. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen für als Phishing-E-Mails identifizierte Nachrichten

auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.4 Sender Policy Framework (SPF)

Der SPF-Filter basiert auf dem Community-Konzept, wobei die Absender ihre Mail-Server in einem SPF-Datensatz mitteilen. Dieser Filter erkennt gefälschte Absender.

- **Beispiel:** Wird eine E-Mail von xyz@companyABC.com gesendet, muss companyABC.com einen SPF-Datensatz veröffentlichen, damit der SPF-Filter erkennen kann, ob die E-Mail tatsächlich über das Netzwerk von companyABC.com versendet wurde oder der Absender gefälscht ist. Wenn kein SPF-Datensatz durch CompanyABC.com veröffentlicht wurde, meldet SPF als Ergebnis 'unknown'.

Weitere Informationen über SPF und dessen Funktionen finden Sie auf der Sender Policy Framework Site unter: http://www.openspf.org.

Der SPF-Filter ist standardmäßig NICHT aktiviert und sollte nur aktiviert werden, wenn Sie glauben, dass die Gefahr gefälschter Absender hoch ist.

GFI MailEssentials verlangt nicht die Veröffentlichung von SPF-Datensätzen. Nutzen Sie zur Veröffentlichung von SPF-Datensätzen den SPF-Assistenten unter:

http://www.openspf.org/wizard.html.

Voraussetzungen

Führen Sie folgende Schritte aus, bevor Sie den SPF-Filter bei einer Serverinstallation ohne Gateway aktivieren:

1. Klicken Sie mit der rechten Maustaste auf **Anti-Spam ► Anti-Spam-Filter ► Eigenschaften** und dann auf die Registerkarte **Perimeter SMTP-Server**.

2. Klicken Sie auf die Schaltfläche **Automatisch erkennen** in der Setup-Option für Perimeter SMTP, eine DNS-MX-Suche durchzuführen und automatisch die IP-Adresse Ihres Perimeter SMTP-Servers zu definieren.

Konfiguration des SPF

1. Wählen Sie: **Anti-Spam ► Anti-Spam-Filter ► Sender Policy Framework ► Eigenschaften**.

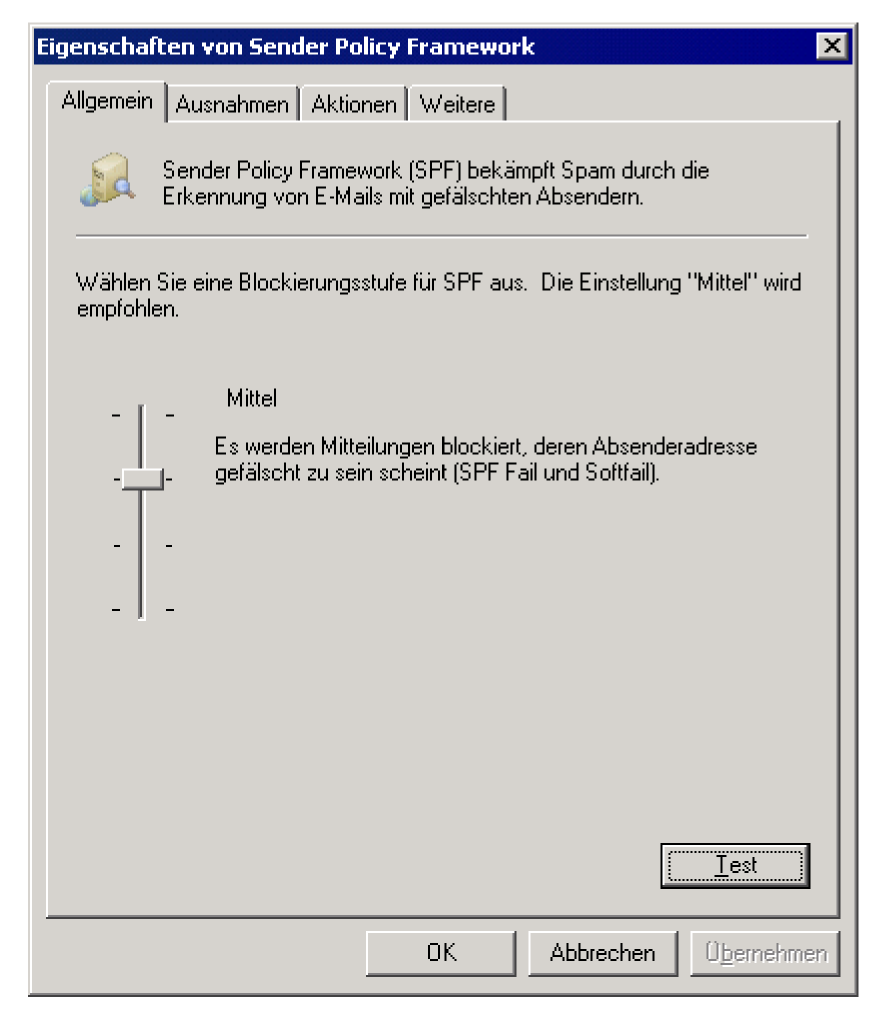


Bild 29 - Konfiguration der SPF-Blockebene

2. Definieren Sie die Empfindlichkeit des SPF-Tests mit dem Schieberegler und klicken Sie auf **Übernehmen**. Wählen Sie eine der vier Ebenen:

- **Keine**: Keine Nachrichten blockieren SPF-Tests werden ignoriert.
- **Liese:** Nur Nachrichten blockieren, deren Absender als gefälscht erkannt wurde. Diese Option behandelt alle Nachrichten mit gefälschten Absendern als Spam.
- **Mittel**: Alle Nachrichten blockieren, die anscheinend einen gefälschten Absender haben. Diese Option behandelt alle Nachrichten als Spam-Mails, die anscheinend von einem gefälschten Absender stammen.

  HINWEIS: Dies ist die Standardeinstellung und empfohlene Einstellung.
- **Hoch:** Alle Nachrichten blockieren, deren Absender nicht nachweislich korrekt ist. Diese Option behandelt alle E-Mails als Spam, sofern nicht nachgewiesen werden kann, dass der Absender nicht gefälscht ist.

  HINWEIS: Da die meisten E-Mail-Server keinen SPF-Datensatz unterstützen, wird diese Option nicht empfohlen.



Bild 30 - Aktuelle Perimeter SMTP-Server-Konfiguration

3. Wenn dieser Computer **NICHT** Ihr Perimeter SMTP-Server ist, wird ein Dialog mit den bereits konfigurierten Perimeter SMTP-Server-Einstellungen angezeigt, (das heißt, die IP-Adressen für Ihren Perimeter SMTP-Server).



Bild 31 - Wichtiger Hinweis: SPF muss auf dem Perimeter SMTP-Server installiert sein.

4. Ist GFI MailEssentials auf Ihrem Perimeter-SMTP-Server installiert oder haben Sie noch nicht angegeben, dass der Mailserver mit GFI MailEssentials KEIN Perimeter-SMTP-Server ist, wird ein Dialog angezeigt. Konfigurieren Sie die Option **Perimeter SMTP-Server** im Anti-Spam-Knoten unter "Eigenschaften" (klicken Sie mit der rechten Maustaste auf die Registerkarte **Anti-Spam ► Anti-Spam Einstellungen ► Eigenschaften ► Perimeter SMTP-Server**.

5. Testen Sie die DNS-Einstellungen/Dienste, indem Sie auf **Testen** klicken.

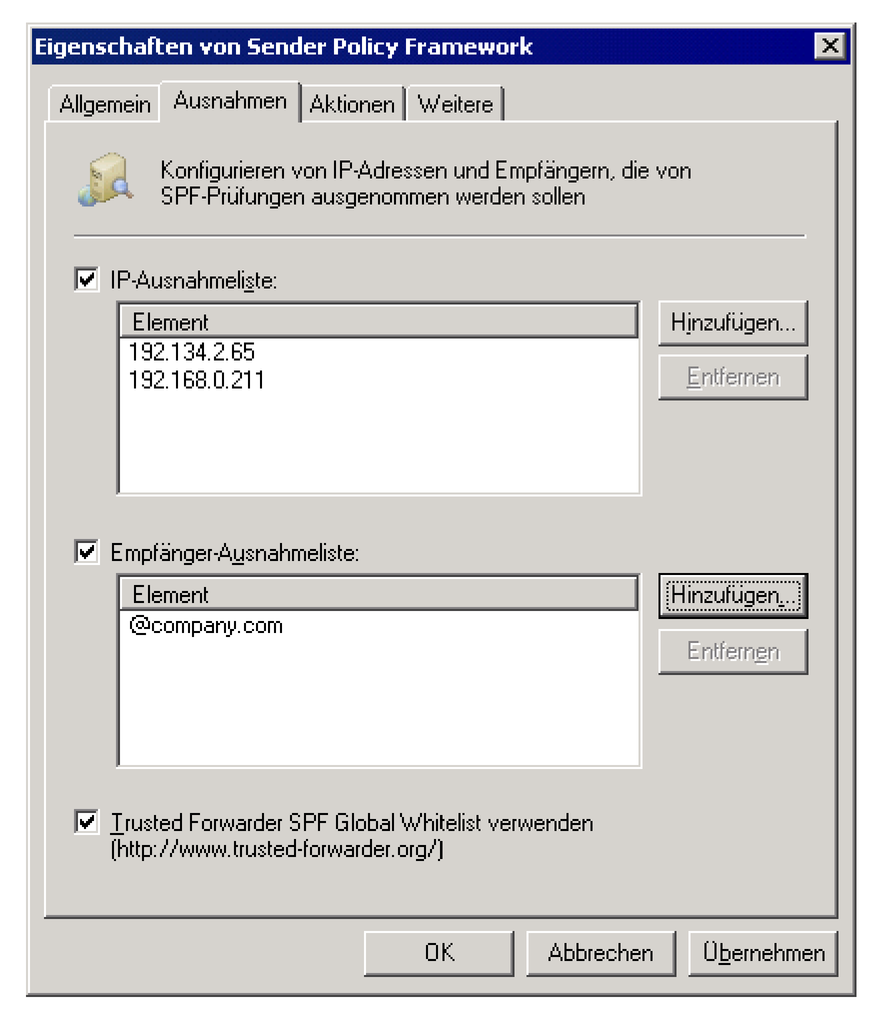


Bild 32 - Konfiguration der SPF-Ausnahmen

6. Klicken Sie auf die Registerkarte **Ausnahmen** um die IP-Adressen und Empfänger zu konfigurieren, die bei den SPF-Prüfungen ausgeschlossen werden sollen:

- **IP-Ausnahmeliste:** Einträge in dieser Liste werden bei den SPF-Prüfungen automatisch übersprungen.

  Klicken Sie auf **Hinzufügen** um eine neue IP-Adresse hinzuzufügen, oder wählen Sie Einträge aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen** um die markierten Einträge zu entfernen. Deaktivieren Sie das Kontrollkästchen IP-Ausnahmeliste, wenn Sie die **IP-Ausnahmeliste** nicht verwenden wollen.

- **Empfänger-Ausnahmeliste:** Mit dieser Option ist gewährleistet, dass bestimmte Empfänger immer E-Mails erhalten, selbst wenn die Nachrichten herausgefiltert wurden. Eine Empfängerausnahme können Sie auf drei Arten eingeben:

  - localpart - 'abuse' (Treffer sind 'abuse@abc.com', 'abuse@xyz.com', usw...)
  - Domäne - '@abc.com' (Treffer sind 'john@abc.com', 'jill@abc.com' usw.....)
  - komplett - 'joe@abc.com' (Treffer ist nur 'joe@abc.com')

  Deaktivieren Sie das Kontrollkästchen **Empfänger-**

Ausnahmeliste, wenn Sie die Empfänger-Ausnahmeliste nicht verwenden wollen.

- **Globale Trusted Forwarder SPF-Whitelist:** http://www.trusted-forwarder.org/Diese Whitelist (www.trusted-forwarder.org) enthält eine globale Whitelist für SPF-Benutzer. Auf diese Weise werden zulässige E-Mails erlaubt, die über bekannte vertrauenswürdige E-Mail-Versender versendet wurden.

  HINWEIS: Standardmäßig ist diese Einstellung aktiviert. Wir empfehlen, diese Option immer aktiviert zu lassen.

7. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen für als Phishing-E-Mails identifizierte Nachrichten auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

8. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.5 Whitelist

Die Whitelistist ist eine Liste der E-Mail-Adressen und Domänen, von denen immer E-Mails empfangen werden dürfen. E-Mails von diesen E-Mail-Adressen oder Domänen werden niemals als Spam-Mails markiert. Es können auch Keywords konfiguriert werden, die, wenn sie im Nachrichtentext oder in der Betreffzeile gefunden werden, die E-Mail automatisch in die Whitelist eintragen.

GFI MailEssentials besitzt auch eine automatische Whitelist-Option, die automatisch E-Mail-Adressen in Whitelists einträgt, wenn an diese E-Mails versendet werden. Auf diese Weise wird der Empfang von E-Mails der Absender erlaubt, an die E-Mails gesendet wurden.

Die Whitelist-Funktion und die Auto-Whitelist-Funktion sind nach Installation von GFI MailEssentials standardmäßig aktiviert.

Wichtige Hinweise

1. Wir empfehlen unbedingt die Auto-Whitelist-Funktion aktiviert zu lassen, da damit ein Großteil der falsch-positiven Erkennungen verhindert wird.

2. Wenn Sie zu viele Keywords eingeben, erhöht sich die Wahrscheinlichkeit, dass Spam-Mails die Spam-Filter passieren.

Konfiguration der Whitelist

1. Wählen Sie **Anti-Spam ► Whitelist ► Eigenschaften.**

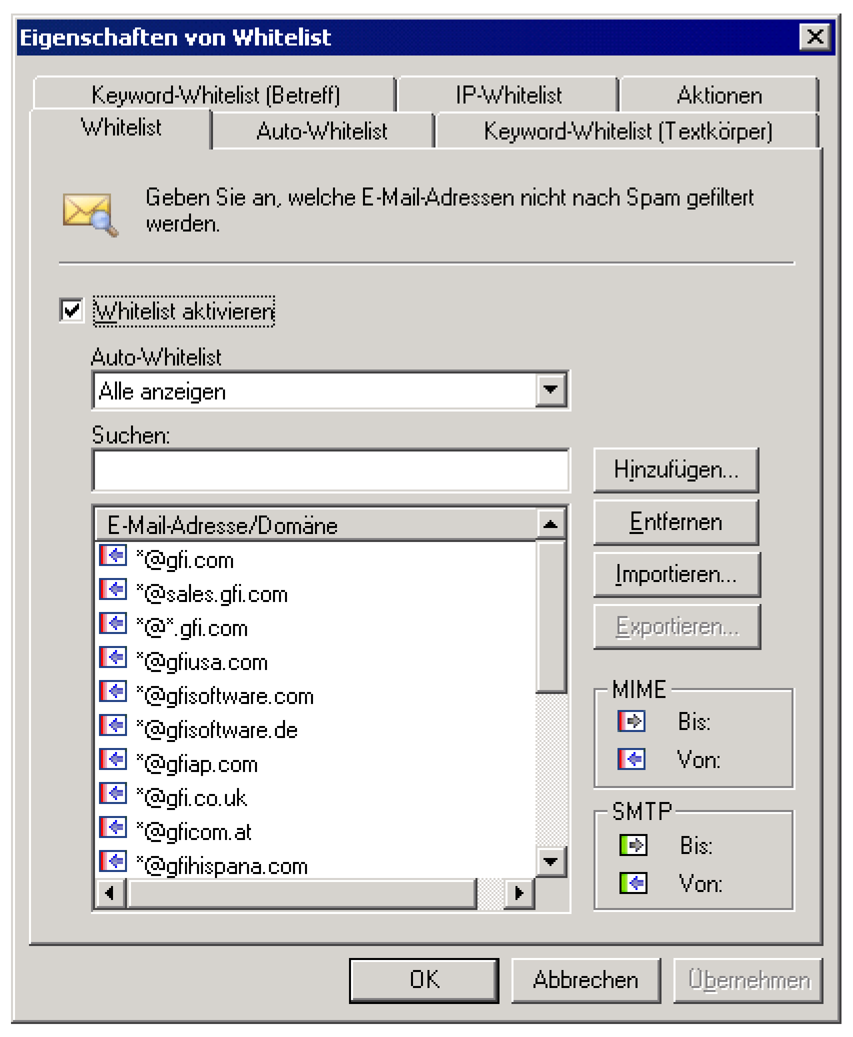


Bild 33 - Whitelist-Domänen

2. Ergänzen Sie über die Registerkarte **Whitelist** eine Domäne oder E-Mail-Adresse in der Whitelist, indem Sie auf **Hinzufügen** klicken.

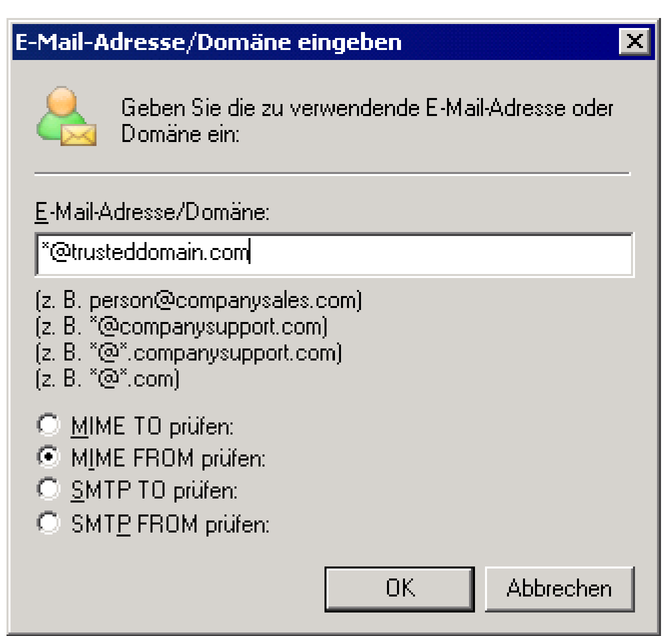


Bild 34 - Hinzufügen einer E-Mail in der Whitelist

3. Geben Sie in dem Dialog **E-Mail-Adresse/Domäne eingeben** folgendes ein:

- Vollständige E-Mail-Adresse oder
- E-Mails einer bestimmten Domäne (Beispiel:) *@companysupport.com); oder
- Einen kompletten Domänen-Suffix (Beispiel:) *@*.mil oder *@*.edu)

  HINWEIS: Wenn Sie einen kompletten Domänensuffix konfigurieren ist beispielsweise gewährleistet, dass E-Mails von Universitäten oder vom Militär nie als Spam markiert werden.

Geben Sie außerdem an, welches E-Mail-Header-Feld mit den E-Mails übereinstimmen muss, die in der Whitelist eingetragen werden, wenn Sie auf **Prüfen …** klicken.

- **Beispiel:** Um alle von einem bestimmten Benutzer eingehenden E-Mails in die Whitelist einzutragen, wählen Sie die Option **MIME FROM:** prüfen.

HINWEIS 1: Einige Newsletter verwenden Mailprogramme, die den Sender nicht in dem Feld MIME FROM eintragen, sodass bei der Prüfung des Headers durch GFI MailEssentials diese Newsletter als Spam markiert werden. Diese Newsletter sollten über die Option **MIME TO:** geprüft werden.

HINWEIS 2: Damit ein lokaler Benutzer nicht durch den Spam-Filter geprüft wird, geben Sie einfach die E-Mail-Adresse des Benutzers ein, und klicken dann auf **MIME TO:** prüfen.

Klicken Sie auf **OK** um die eingetragene E-Mail/Domäne zu übernehmen.

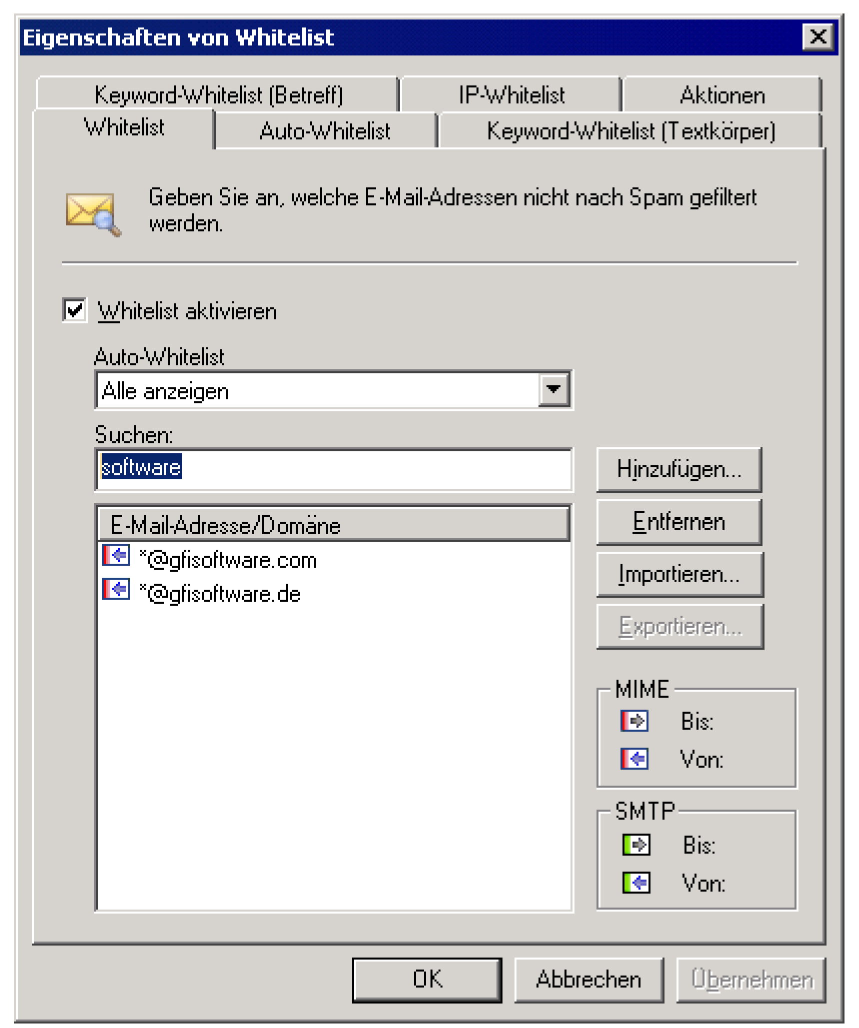


Bild 35 - E-Mail-Adressen und Mails der Whitelist suchen

4. Um in der Whitelist E-Mail-Adressen und Domänen zu suchen, geben Sie ein Suchkriterium in dem Textfeld **Suchen** ein. Passende Einträge werden automatisch darunter angezeigt.

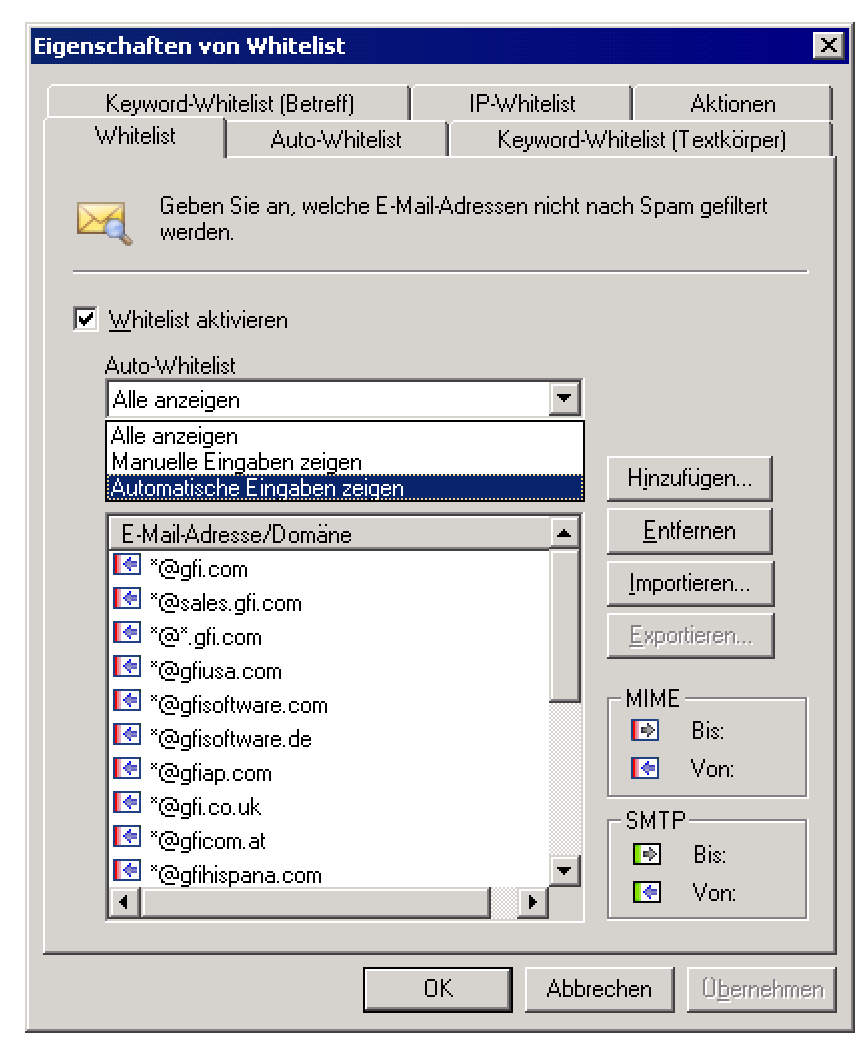


Bild 36 - Optionen für die automatische Whitelist

5. Klicken Sie auf die Registerkarte **Automatische Whitelist**, um die folgenden Optionen für die automatische Whitelist zu konfigurieren:

- **Automatische Whitelist automatisch füllen:** Wenn Sie diese Option wählen, werden die Empfängeradressen abgehender E-Mails automatisch in die Whitelist eingetragen.
- **Maximal zulässige Zahl der Einträge in der Whitelist:** Geben Sie die Anzahl der Einträge an, die in der automatischen Whitelist zulässig sind. Wenn dieses angegebene Limit überschritten wird, werden die ältesten Einträge automatisch durch die neuen Einträge ersetzt.
- **Automatische Whitelist für E-Mails aktivieren:** Wenn Sie diese Option auswählen, werden eingehende E-Mails gescannt und die Absender mit der Whitelist verglichen. Wenn der Absender in der Liste enthalten ist, wird die E-Mail direkt in das Empfängerpostfach weitergeleitet.

HINWEIS: Einträge in der automatischen Whitelist können Sie in der Registerkarte **Whitelist** anzeigen, wenn Sie auf die Option "Automatische Einträge anzeigen" in dem Dropdown-Feld **Whitelist-Einträge filtern** klicken.

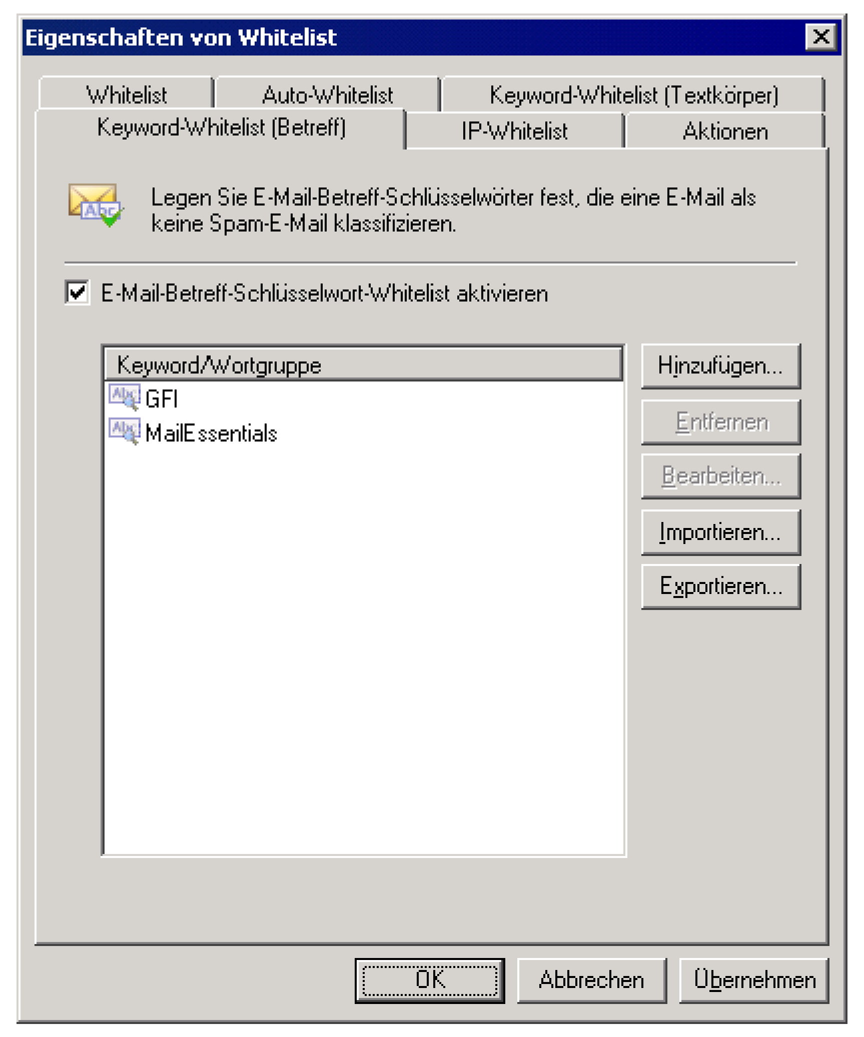


Bild 37 - Whitelist-Keywords

6. Klicken Sie auf die Registerkarte **Keyword-Whitelist** (Betreff) oder Keyword-Whitelist (Nachrichtentext) um die Keywords anzugeben, die E-Mails als HAM (zulässige E-Mail) markieren, sodass die E-Mail automatisch von den Spam-Filtern ignoriert wird. Definieren Sie neue Keywords, indem Sie auf die Schaltfläche **Hinzufügen** klicken oder mit den Schaltflächen **Entfernen**, **Bearbeiten**, **Importieren** und **Exportieren** die vorhandenen Keywords verändern.

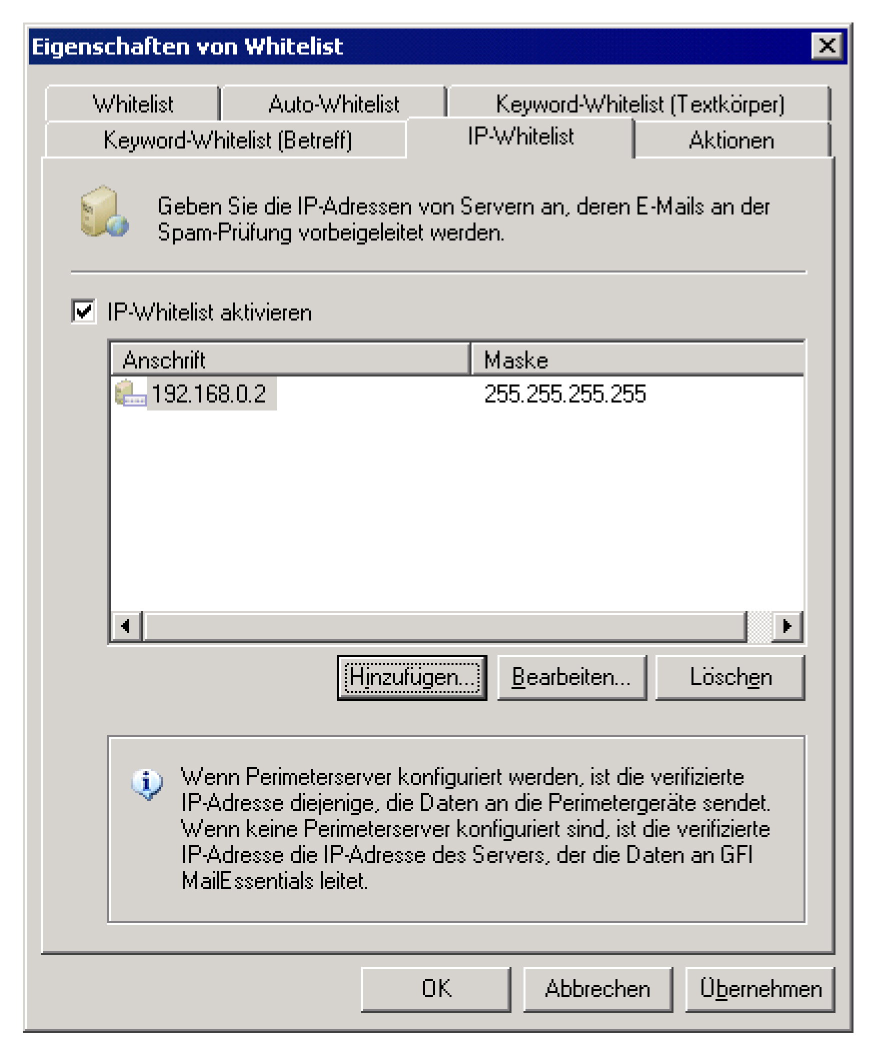


Bild 38 - Whitelist IPs

7. Klicken Sie auf die Registerkarte **IP Whitelist**, um automatisch E-Mails von bestimmten IP-Adressen anzuzeigen. Aktivieren Sie diese Funktion, indem Sie die Option **IP Whitelist aktivieren** auswählen und auf die Schaltfläche **Hinzufügen** klicken, um eine einzelne IP-Adresse oder eine Subnetzmaske einzugeben, bei der die Spamprüfungen übergangen werden sollen.

8. Klicken Sie auf die Registerkarte **Aktionen**, um die Protokollierung der Whitelist in einer Datei zu aktivieren oder zu deaktivieren. Klicken Sie auf **Durchsuchen**, um einen Ordner anzugeben, in dem die Protokolle gespeichert werden sollen.

9. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.6 Directory Harvesting

Directory Harvesting-Angriffe nutzen bekannte E-Mail-Adressen als Vorlage um weitere E-Mail-Adressen zu erzeugen, die dann an Firmen- oder ISP-E-Mail-Server gesendet werden. Die Spammer senden nach dem Zufallsprinzip erzeugte E-Mail-Adressen; zwar können einige E-Mail-Adressen mit echten E-Mail-Adressen übereinstimmen, die Mehrzahl dieser Adressen ist jedoch ungültig und überlastet den E-Mail-Server des Opfers.

GFI MailEssentials stoppt diese Angriffe, indem E-Mails an Benutzer,

die nicht in Active Directory oder im E-Mail-Server des Unternehmens eingetragen sind, blockiert werden.

Directory Harvesting kann entweder so konfiguriert werden, dass die Funktion ausgeführt wird, sobald die vollständige E-Mail empfangen wird (Transport Sink) oder auf SMTP-Ebene, das heißt, beim Empfang der IP des Absenders der E-Mail und der Empfänger (SMTP Protocol Sink). Bei einer SMTP-Filterung wird die E-Mail-Verbindung beendet und damit ein komplettes Herunterladen der E-Mail verhindert um Bandbreite und Verarbeitungskapazität zu sparen. In diesem Fall wird die Verbindung sofort unterbrochen und die E-Mails müssen nicht weitere Spam-Filter passieren.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials NICHT aktiviert.

Konfiguration von Directory Harvesting

Directory harvesting konfigurieren Sie in zwei Phasen:

Phase 1 - Konfiguration der Eigenschaften von Directory Harvesting

Phase 2 - Auswahl des Verfahrens für Directory Harvesting

Phase 1 - Konfiguration der Eigenschaften von Directory Harvesting

1. Klicken Sie auf **Anti-Spam** ► **Anti-Spam-Filter** ► **Directory Harvesting** ► Eigenschaften und dann auf die Option **Schutz vor Directory Harvesting** aktivieren.

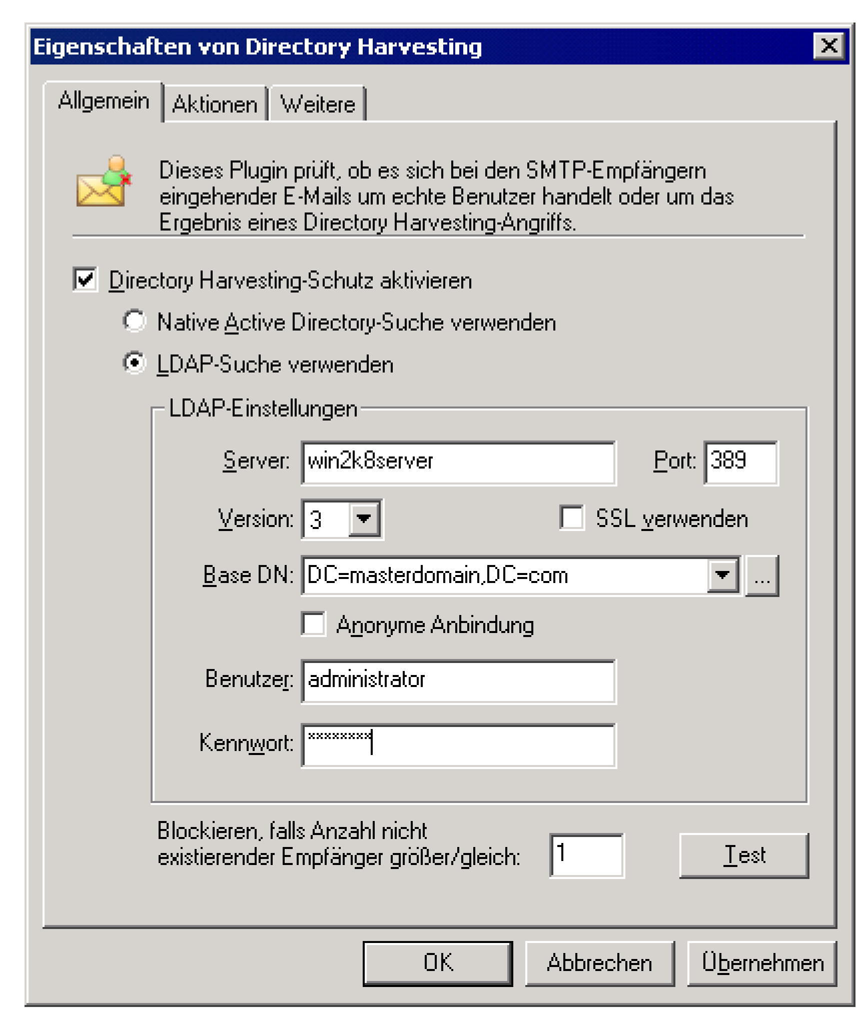


Bild 39 - Die Funktion Directory Harvesting

2. Wählen Sie das gewünschte Suchverfahren aus:

- **Verwenden Sie die Option Native Active Directory-Suche**, wenn GFI MailEssentials im Active Directory-Benutzermodus installiert ist.

  HINWEIS 1: Ist GFI MailEssentials im Active Directory-Benutzermodus in einer DMZ installiert, enthält die Active Directory der DMZ in der Regel nicht alle Netzwerkbenutzer (E-Mail-Empfänger). Nutzen Sie in diesem Fall für Directory Harvesting die LDAP-Suche.

  HINWEIS 2: Befindet sich GFI MailEssentials vor einer Firewall, kann mit der Funktion Directory Harvesting aufgrund der Firewall-Einstellungen möglicherweise keine direkte Verbindung mit dem internen Active Directory aufgebaut werden. Stellen Sie die Verbindung mit dem internen Active Directory Ihres Netzwerks über LDAP her und kontrollieren Sie, ob in Ihrer Firewall der Standard-Port 389 offen ist.

- **Konfigurieren Sie mit "LDAP Suche verwenden"** die LDAP-Einstellungen, wenn GFI MailEssentials im SMTP-Modus installiert ist. Benötigt Ihr LDAP-Server eine Authentifizierung, deaktivieren Sie die Option **Anonyme Bindung** und geben Sie die Authentifizierungsdaten für diese Funktion ein. Klicken Sie auf die Schaltfläche **Testen** um Ihre LDAP-Konfigurationseinstellungen zu

testen.

HINWEIS 1: Definieren Sie die Authentifizierungsdaten im Format Domäne\Benutzer, beispielsweise Master-Domäne\Administrator.

HINWEIS 2: In Active Directory ist der LDAP-Server in der Regel der Domänen-Controller.

3. Geben Sie bei der Option **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich** an, wie viele nicht existierende Empfänger erfasst werden müssen, damit die E-Mail als Spam eingestuft wird. Ist die Gesamtzahl der Empfänger geringer als die angegebene Zahl, wird die konfigurierte Aktion nur ausgelöst, wenn KEINER der Empfänger existiert, anderenfalls wird die E-Mail nicht als Spam gekennzeichnet.

HINWEIS: Vermeiden Sie falsch-positive Treffer, indem Sie eine angemessene Anzahl in dem Bearbeitungsfeld **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich:** eintragen. Bei diesem Wert sollten Sie berücksichtigen, dass Benutzer zulässige E-Mails an mit Tippfehler eingegebene E-Mail-Adressen senden können oder an Benutzer, die nicht mehr im Unternehmen beschäftigt sind.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

HINWEIS: Wenn die Option Directory Harvesting auf SMTP Protocol Sink eingestellt ist, wird nur die Option **Häufigkeit in dieser Datei protokollieren** auf der Registerkarte **Aktionen** angezeigt.

Phase 2 - Auswahl des Verfahrens für Directory Harvesting

1. Klicken Sie auf **Antispam ► Filterpriorität ► Eigenschaften** und dann auf den Knoten **SMTP-Sendefilter**.

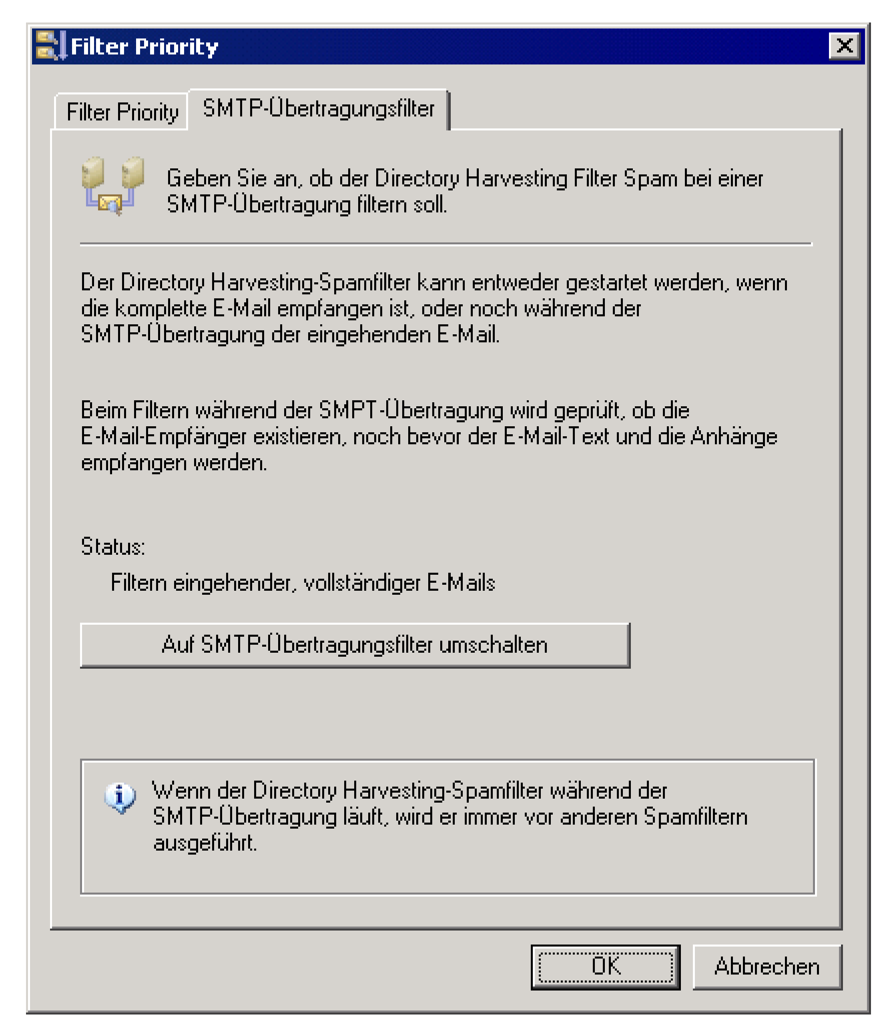


Bild 40 - Der Dialog "Anti-Spam-Reihenfolge"

2. Klicken Sie auf die Schaltfläche, um zwischen folgenden Optionen umzuschalten:

- **Vollständige E-Mail-Filterung** - Die Filterung erfolgt, wenn die gesamte E-Mail empfangen ist.
- **SMTP-Versandfilter** - Die Filterung erfolgt während der SMTP-Übertragung, indem geprüft wird, ob die E-Mail-Empfänger existieren, bevor der Nachrichtentext und die Anhänge empfangen werden.

  HINWEIS: Wenn Sie diese Option auswählen, wird die Option "Directory Harvesting" immer vor anderen Spamfiltern gestartet.

3. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.7 E-Mail Blacklist

Die Blacklist ist eine Datenbank der E-Mail-Adressen und Domänen, von denen Sie niemals E-Mails empfangen wollen.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Konfiguration benutzerdefinierter Blacklists

Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► E-Mail Blacklist**

► **Eigenschaften.**

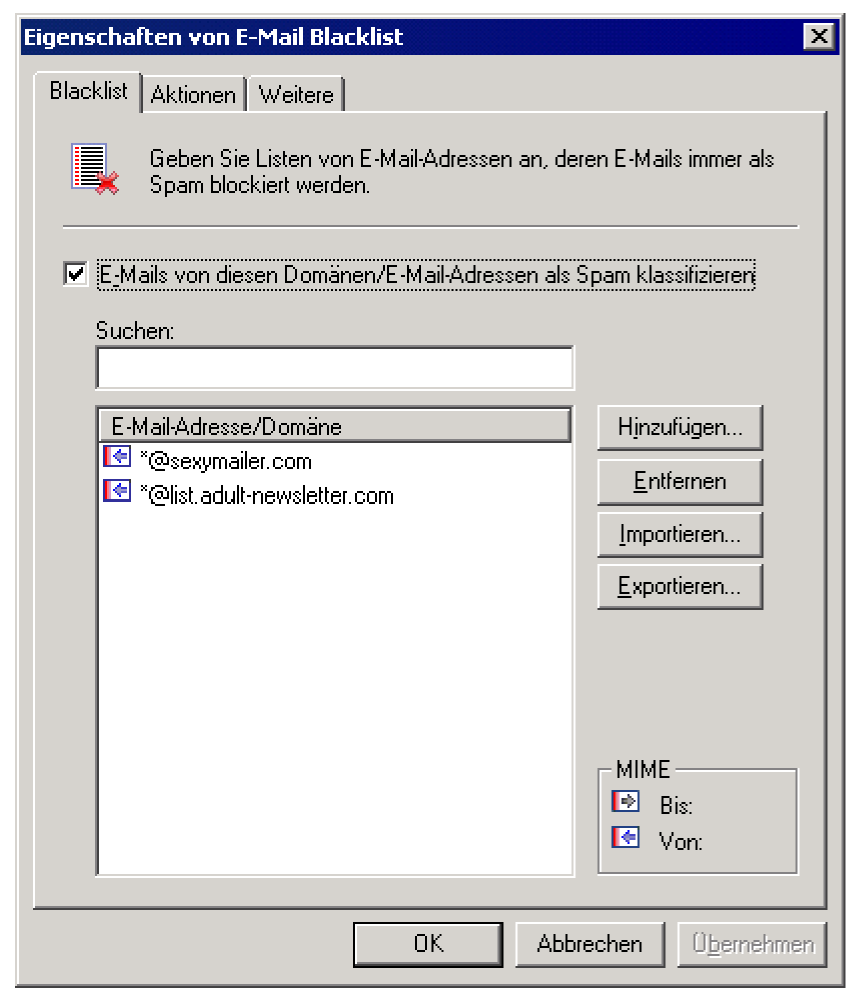


Bild 41 - Die benutzerdefinierte Blacklist

2. Klicken Sie auf **Hinzufügen** um eine Domäne oder eine E-Mail-Adresse der Blacklist hinzuzufügen.

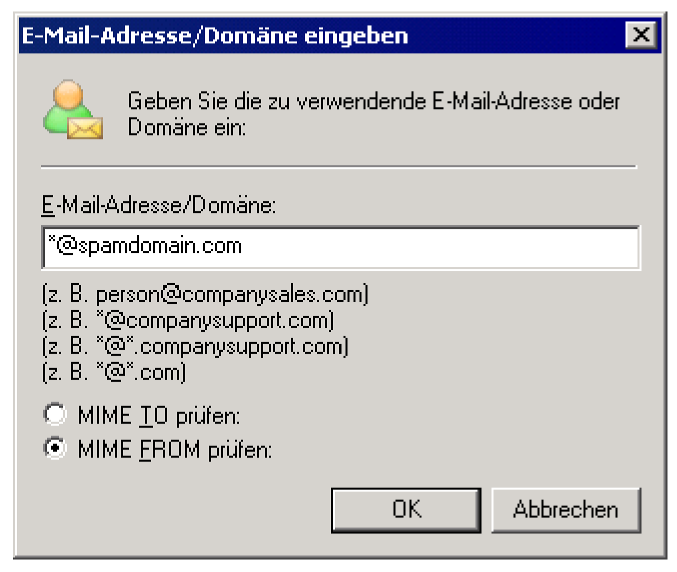


Bild 42 - Hinzufügen einer E-Mail zur Blacklist

3. Geben Sie im Dialog **E-Mail-Adresse/Domäne eingeben** die vollständige E-Mail-Adresse oder die komplette Domäne ein (Beispiel: *@spammer.com) oder einen Suffix für eine komplette Domäne (Beispiel: *@*.tv). Geben Sie außerdem an, welches E-Mail-Header-Feld mit den E-Mails in der Blacklist übereinstimmen muss, indem Sie auf das Feld **MIME TO prüfen:** oder **MIME FROM prüfen:** klicken.

4. Um in der Blacklist der E-Mail-Adressen und Domänen zu suchen, geben Sie ein Suchkriterium in dem Textfeld **Suchen** ein. Passende Einträge werden automatisch darunter angezeigt.

5. Klicken Sie auf die Registerkarte **Aktionen** bzw. **Weitere** um die Aktionen für Spam-Nachrichten auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.8 Bayes'sche Analyse

Der Bayes-Filter ist ein Spam-Filter in GFI MailEssentials, bei dem adaptive Verfahren mit Algorithmen künstlicher Intelligenz genutzt werden um möglichst viele der heute üblichen Spam-Verfahren zu erkennen.

Weitere Informationen über den Bayes-Filter, dessen Konfiguration und Training finden Sie in Anhang 2 - Einsatz des Bayes-Filter auf Seite 143 in diesem Handbuch.

HINWEIS: Der Bayes-Filter ist standardmäßig deaktiviert.

WICHTIGER HINWEIS: Der Bayes-Filter erreicht seine maximale Leistung frühestens nach einer Woche nach seiner Aktivierung. Diese Zeit ist erforderlich, weil der Bayes-Filter seine Höchsterkennungsrate nur dann erreicht, wenn er sich an Ihre E-Mail-Muster anpasst.

Konfiguration des Bayes-Filters

Die Konfiguration des Bayes-Filters erfordert zwei Phasen:

Phase 1: Konfiguration des Bayes-Filters

Phase 2: Aktivierung des Bayes-Filters

Phase 1: Konfiguration des Bayes-Filters

Der Bayes-Filter Bayes-Filter kann auf zwei Arten trainiert werden:

1. Automatisch durch ausgehende E-Mails.

GFI MailEssentials erfasst zulässige E-Mails (HAM) durch Scannen der ausgehenden E-Mails. Der Bayes-Filter kann aktiviert werden, sobald mindestens 500 ausgehende E-Mails gesammelt wurden (wenn Sie nur englische E-Mails versenden) oder mindestens 1000 ausgehende E-Mails (wenn Sie E-Mails nicht in Englisch versenden).

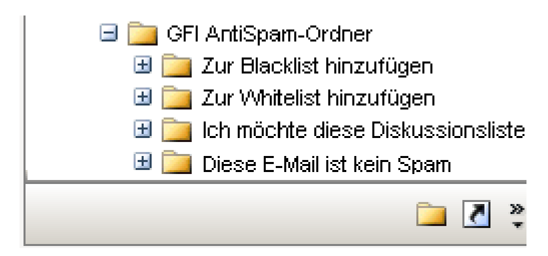


Bild 43 - Training des Bayes-Filters mit zulässigen E-Mails

2. Manuelles Training mit vorhandenen E-Mails

Kopieren Sie 500 bis 1000 E-Mails aus Ihrem Versandordner in den Unterordner **Das sind zulässige E-Mails** in die **Anti-Spam folders** (öffentlichen Ordner) um den Bayes-Filter genauso zu trainieren wie beim Versand von E-Mails.

Phase 2: Aktivierung des Bayes-Filters

Sobald der Bayes-Filter trainiert ist, muss er aktiviert werden.

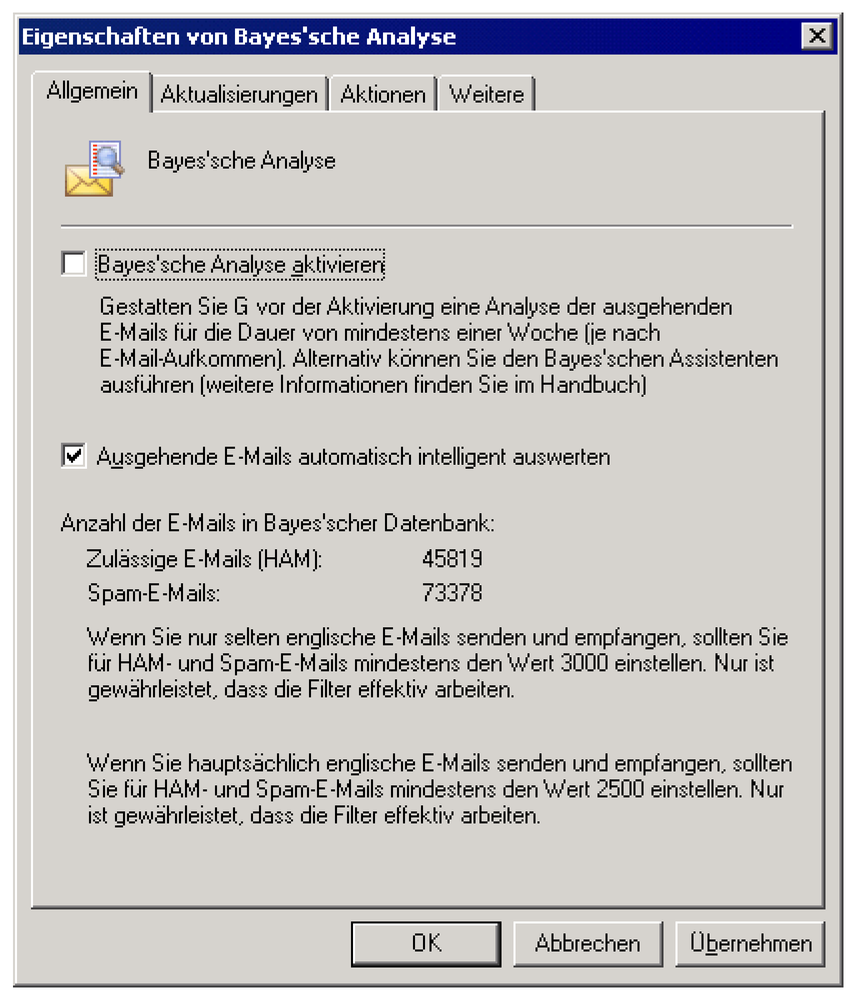


Bild 44 - Bayes-Filter-Analyseeigenschaften

1. Klicken Sie in der Konfigurationskonsole von GFI MailEssentials auf **Anti-Spam** ► **Anti-Spam-Filter** ► **Bayes-Analyse** ► **Eigenschaften.** Klicken Sie auf der Registerkarte **Allgemein** auf das Kontrollkästchen Bayes-Analyse aktivieren.

2. Achten Sie darauf, dass die Option **Automatisch mit**

ausgehenden E-Mails trainieren aktiviert ist. Damit wird die Datenbank zulässiger E-Mails zulässige E-Mails laufend mit den Daten ausgehender E-Mails aktualisiert.

3. Konfigurieren Sie auf der Registerkarte **Aktualisierungen** die Häufigkeit der Aktualisierungen für die Spam-Datenbank, indem Sie die Option **Automatisch nach Aktualisierungen suchen** aktivieren und ein Intervall in Stunden angeben.

HINWEIS 1: Klicken Sie auf die Schaltfläche **Aktualisierungen jetzt herunterladen** um sofort Aktualisierungen herunterzuladen.

HINWEIS 2: Weitere Informationen zur Auswahl der bevorzugten Server sowie zum Herunterladen von Updates mit einem Proxyserver finden Sie unter Konfigurieren automatischer Updates Auf Seite 120 in diesem Handbuch

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.9 DNS-Blacklists (DNSBL)

GFI MailEssentials unterstützt verschiedene DNS-Blacklists. Diese SMTP-Server-Datenbanken enthalten Listen von Servern, die für Spam-Aktionen verwendet wurden. Es gibt verschiedene DNS-Blacklists von Drittanbietern, die sehr zuverlässig sein können, weil sie klar definierte Prozeduren für die Aufnahme und Aussonderung aus der DNS-Blacklist verwenden, aber auch weniger zuverlässige Listen.

Wenn eine E-Mail von einem Absender an den Empfänger gesendet wird, wird sie über eine Reihe von SMTP-Servern übertragen, bis sie ihr Ziel erreicht. Im E-Mail-Header wird die IP-Adresse jedes SMTP-Servers vermerkt. Mit diesem Filter kann GFI MailEssentials alle öffentlichen IP-Adressen im Nachrichten-Header prüfen und mit der konfigurierten DNSBL-Datenbank vergleichen.

GFI MailEssentials prüft alle in den Nachrichten-Header enthaltenen öffentlichen IP-Adressen auf Vorhandensein in der konfigurierten DNSBL-Datenbank. GFI MailEssentials speichert alle geprüften IP-Adressen in einer internen Datenbank und führt für die gleichen IP-Adressen mit der DNS-BL keine weiteren Prüfungen durch. Die IP-Adressen werden vier Tage lang in der Datenbank gehalten bzw. bis das SMTP-Protokoll neu gestartet wird.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Wichtige Hinweise

1. Der DNS-Server muss korrekt konfiguriert sein, damit diese Funktion zur Verfügung steht. Ist dies nicht der Fall, kommt es zu einem Zeitüberlauf, und der E-Mail-Traffic wird verzögert. Weitere Informationen dazu finden Sie unter http://kbase.gfi.com/showarticle.asp?id=KBID001770.

2. Die Abfrage einer DNS-Blacklist kann eine gewisse Zeit erfordern

(je nach Ihrer Verbindung), sodass E-Mails etwas verzögert werden, insbesondere wenn mehrere DNS-Blacklists abgefragt werden.

Konfiguration der DNSBL

1. Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► DNS-Blacklists ► Eigenschaften**.

2. Aktivieren Sie das Kontrollkästchen **Mail-Server auf Eintrag in einer der folgenden DNS-Blacklists überprüfen:**

3. Wählen Sie die entsprechenden DNS-Blacklists aus um eingehende E-Mails zu prüfen und klicken Sie auf die Schaltfläche **Testen** um zu kontrollieren, ob die ausgewählten Blacklists verfügbar sind.

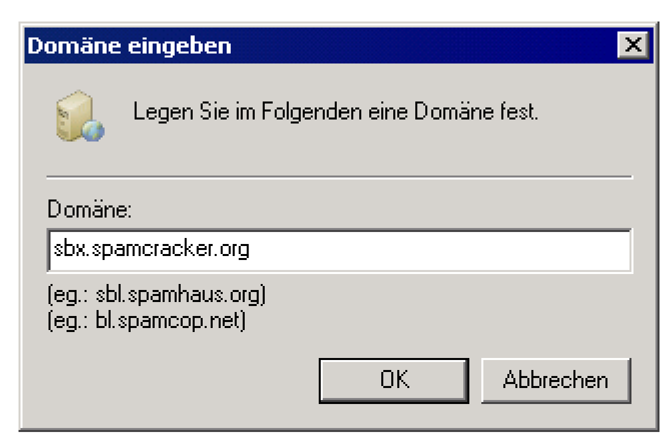


Bild 45 - Hinzufügen weiterer DNS-Blacklists

4. Bei Bedarf können Sie weitere DNS-Blacklists zu den bereits in der Liste aufgeführten hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** klicken und die Domäne mit der DNSBL eingeben.

HINWEIS: Die Referenzreihenfolge für eine aktivierte DNS-Blacklist können Sie ändern, indem Sie eine Blacklist auswählen und dann auf die Schaltflächen **Aufwärts** bzw. **Abwärts** klicken.

5. Wählen Sie die Option **E-Mails von dynamischen IP-Adressen in SORBS.net blockieren** aus, damit GFI MailEssentials Spam-Mails von Botnet/Zombies erkennen kann. Dazu vergleicht GFI MailEssentials die eingehende Verbindungs-IP mit bekannten Botnet-/Zombie-IP-Adressen in der Sorbs.net-Datenbank.

6. Klicken Sie auf **Übernehmen** um die Konfiguration zu speichern.



Bild 46 - Aktuelle Perimeter SMTP-Server-Konfiguration

7. Ist dieser Computer **NICHT** Ihr SMTP-Server, erscheint ein Dialog mit den Perimeter SMTP-Server-Einstellungen, die Sie im GFI

MailEssentials konfiguriert haben (das heißt, mit den IPs für Ihren Perimeter SMTP-Server).



Bild 47 - Wichtiger Hinweis: SPF muss auf dem Perimeter SMTP-Server installiert sein .

7. Befindet sich diese Installation auf einem SMTP-Server oder ist der Mail-Server mit GFI MailEssentials noch nicht angegeben, erinnert Sie ein Dialog daran, dass dieser Computer nicht der Perimeter-Server ist.

8. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

9. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.10 Spam URI Realtime Blocklists (SURBL)

Ein Uniform Resource Identifier (URI) ist ein Standard für den Zugriff auf Ressourcen im Web. Übliche URIs wie die URLs (Web-Adressen) und Uniform Resource Names (URNs) dienen zur Identifizierung des Ziels für Hypertext-Links sowie der Quellen von Bildern, Daten und anderen Objekten auf einer Website. URLs werden häufig bei Websites verwendet, können aber auch Teil einer E-Mail-Nachricht sein.

SURBLs unterscheiden sich von den meisten anderen RBLs dadurch, dass mit ihnen Spam-Mails anhand der URIs in der Textnachricht erkannt werden können. Im Gegensatz zu den meisten anderen RBLs werden SURBLs nicht verwendet um Spam-Absender zu blockieren. Stattdessen können sie Nachrichten blockieren, in deren Text Spam-Hosts, beispielsweise Web-Server, Domänen und Websites, enthalten sind.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Konfiguration der Spam URI Realtime Blocklists

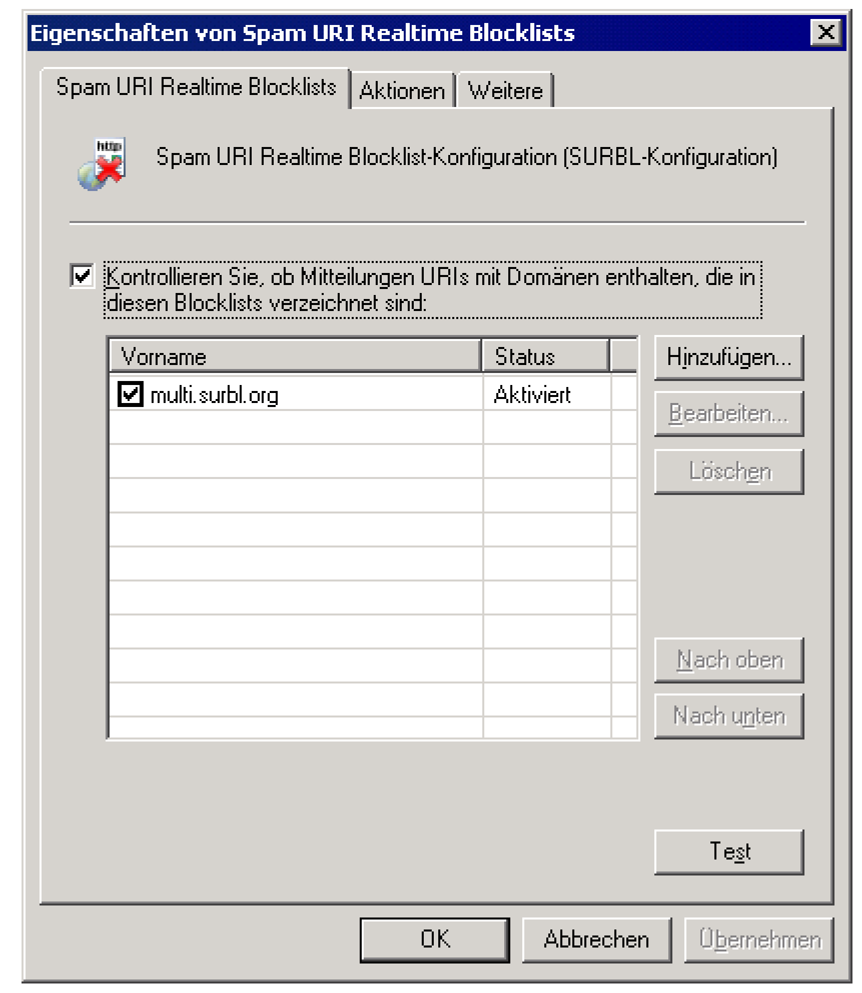


Bild 48 - Spam URI Realtime Blacklist - Eigenschaften

1. Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► Spam URI Realtime Blocklists ► Eigenschaften**.

2. Klicken Sie auf die Registerkarte "Spam URIRealtime Blacklist":

- Aktivieren/Deaktivieren Sie die Option **Nachricht auf URIs mit Domänen folgender Blacklists prüfen:** um diese Funktion zu aktivieren/deaktivieren.
- Wählen Sie aus der verfügbaren Liste die Blacklists aus, die als Referenz verwendet werden sollen, wenn Sie Nachrichten mit der SURBL-Funktion SURBL prüfen.
- Klicken Sie auf die Schaltfläche **Hinzufügen** um weitere SURBLs hinzuzufügen.

Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Testen** und klicken Sie auf **Übernehmen** um die Einstellungen zu speichern.

HINWEIS 1: Definieren Sie den vollständigen Namen der Domäne (beispielsweise URIBL.com) mit der Blacklist.

HINWEIS 2: Multi.surbl.org kombiniert folgende Listen zu einer einzigen Liste:

- sc.surbl.org
- ws.surbl.org

- Phishing-Datenquelle von mailsecurity.net.au
- Phishing-Datenquelle von fraud.rhs.mailpolice.com
- ob.surbl.org
- ab.surbl.org
- jp data source

Deaktivieren Sie alle anderen SURBL-Listen, wenn Sie multi.surbl.org aktivieren, da sonst die E-Mail-Bearbeitungszeit verlängert wird.

Bei vielen falsch-positiven Treffern sollten Sie multi.surbl.org deaktivieren und die anderen SURBL-Listen aktivieren.

Weitere Informationen zu SURBL-Listen finden Sie unter http://www.surbl.org/lists.html.

5. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.11 Header-Prüfung

Der Filter "Header-Prüfung" analysiert die einzelnen Felder in einem Header. Bei diesem Verfahren werden das SMTP- und MIME-Feld genutzt, wobei die SMTP-Felder vom Mail-Server definiert werden und die MIME-Felder vom E-Mail-Client (der die E-Mail in MIME codiert).

Konfiguration der Header-Prüfung

1. Klicken Sie auf **Anti-Spam** ► **Anti-Spam-Filter** ► **Header-Prüfung** ► **Eigenschaften**.

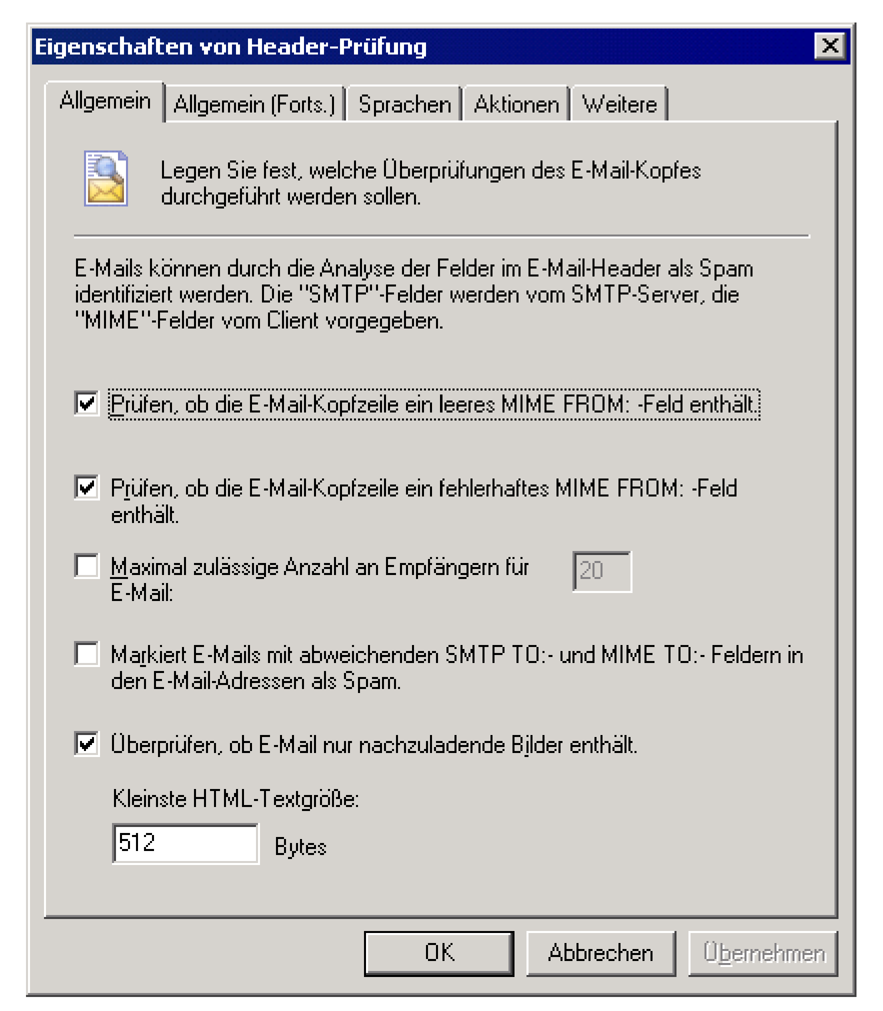


Bild 49 - Registerkarte Header-Prüfung AllgemeinHeader-Prüfung

2. Auf die Registerkarten **Allgemein** und **Allgemein Forts.** können Sie die folgenden Parameter aktiveren, deaktivieren oder konfigurieren.

- **Prüft, ob der E-Mail-Header ein leeres Feld MIME FROM enthält:** Prüft, ob der Absender sich selbst in dem Feld FROM: identifiziert hat. Ist dieses Feld leer, wird die Nachricht als Spam markiert.
- **Prüft, ob der E-Mail-Header ein Feld MIME FROM: enthält:** Prüft, ob das Feld MIME FROM die richtige Notation besitzt (ob der Header mit RFC übereinstimmt).
- **Maximale Anzahl der zulässigen Empfänger in der E-Mail:** Identifiziert E-Mails mit vielen Empfängern und markiert diese als Spam.
- **Markiert E-Mails mit verschiedenen Feldern SMTP TO: und MIME TO: in den E-Mail-Adressen als Spam:** Überprüft, ob die Felder SMTP TO: und MIME TO: identisch sind. Der E-Mail-Server des Spammers muss immer eine Adresse SMTP TO: enthalten. Die Adresse MIME TO: ist jedoch oft nicht enthalten oder weicht ab.

  HINWEIS: Mit dieser Funktion lassen sich viele Spam-Mails identifizieren, allerdings enthalten auch einige Listen-Server das Feld MIME TO: nicht. Wir empfehlen daher, die Absenderadresse

von Newslettern in die Whitelist einzutragen, wenn diese Funktion verwendet werden soll.

- **Überprüfen, ob E-Mail nur nachzuladende Bilder enthält:** Diese Funktion markiert E-Mails als Spam, die nur nachzuladende Bilder und nur minimalen Text enthalten. Diese Funktion identifiziert Spam-Mails, die nur Bilder enthalten.
- **Gültigkeit der Absender-Domäne überprüfen:** Diese Funktion führt eine DNS-Suche in der Domäne durch, die in dem Feld MIME FROM eingetragen ist, und überprüft die Gültigkeit der Domäne.

  HINWEIS: Der DNS-Server muss korrekt konfiguriert sein, damit es nicht zu einem Zeitüberlauf und zu einer Verzögerung der E-Mail-Übertragung kommt. Außerdem kann dieser Filter viele zulässige E-Mails als Spam markieren. Prüfen Sie Ihren DNS-Server und die Dienste, indem Sie auf **Testen** klicken.
- **Maximal zulässige Anzahl in dem Feld MIME FROM:** Identifiziert eine Nachricht bei Existenz von mehr als drei Zahlen in dem Feld MIME FROM als Spam-Nachricht. Spammer nutzen oft Tools, die automatisch Antwortadressen erstellen. Häufig nutzen sie drei oder mehr Ziffern in dem Namen um sicherzugehen, dass die Antwortadresse einmalig ist.
- **Diese Funktion prüft, ob der E-Mail-Betreff den ersten Teil der Empfänger-E-Mail-Adresse enthält:** Diese Funktion identifiziert personalisierte Spam-Mails, bei denen die Spammer häufig den ersten Teil der Empfänger-E-Mail-Adresse in der Betreffzeile einfügen.

  HINWEIS: Achten Sie darauf, dass Sie E-Mail-Adressen, für die diese Prüfung nicht ausgeführt werden soll, durch einen Klick auf die Schaltfläche **Außer …** konfigurieren. Auf diese Weise werden allgemeine E-Mail-Adressen, an die Kunden antworten, beispielsweise E-Mails von sales@company.com mit einem Betreff 'Ihre E-Mail an den Vertrieb', nicht als Spam markiert
- **E-Mail auf codierte IP-Adressen prüfen:** Überprüft den Nachrichten-Header und den Nachrichtentext auf URLs mit einer im Hexa- oder Oktal-Format codierten IP (http://0072389472/hello.com) oder auf eine Kombination aus Benutzername und Kennwort (beispielsweise: www.citibank.com@scammer.com).
  - o Folgende Beispiele würden als Spam gekennzeichnet:
    - *http://12312*
    - *www.microsoft.com:hello%01@123123*
- **E-Mails auf eingebettete GIF-Bilder prüfen:** Prüft, ob die E-Mail mindestens ein eingebettetes GIF-Bild enthält. Eingebettete GIF-Bilder werden oft verwendet um Spam-Filter zu umgehen.

  WICHTIGER HINWEIS: Da einige zulässige E-Mails eingebettete GIF-Bilder enthalten können, liefert diese Option oft falsch-positive Treffer.
- **E-Mail auf Spam-Anhang überprüfen:** Überprüft E-Mail-Anhänge auf Eigenschaften, die bei in Spam-Mails versendeten Dateianhängen häufig sind. Dies ist eines der modernsten

Verfahren, das Spammer einsetzen um über Dateianhänge Spam zu versenden.

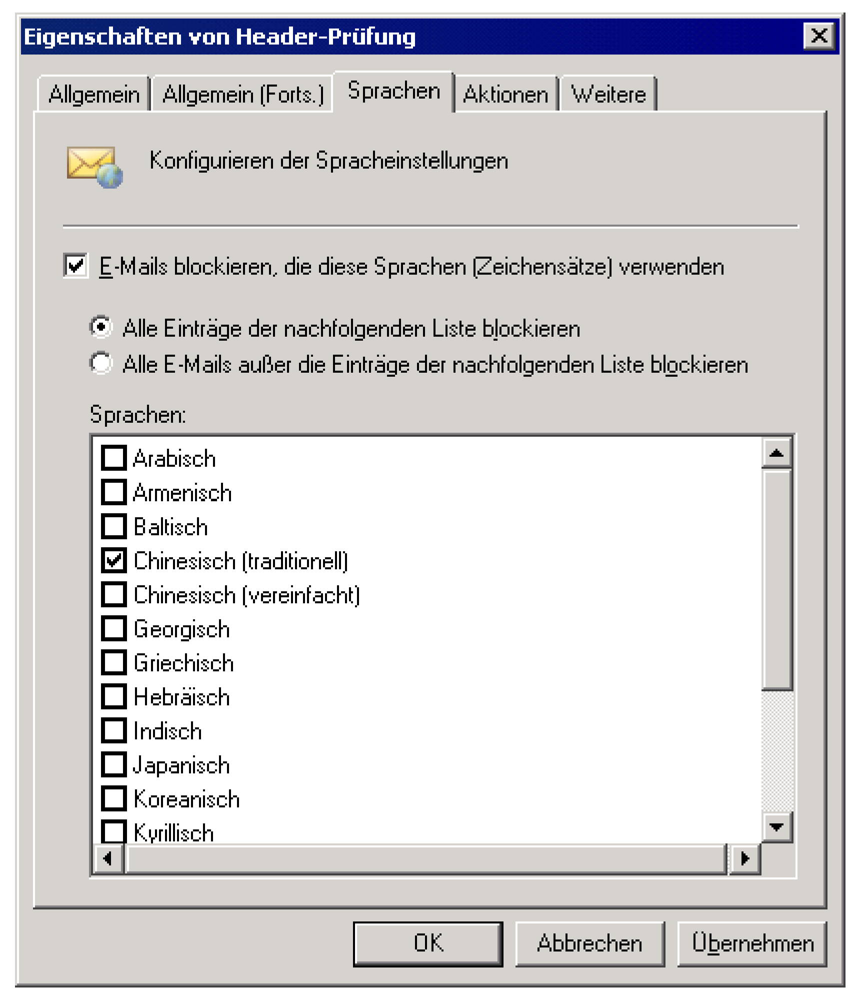


Bild 50 - Spracherkennung

3. Klicken Sie auf der Registerkarte "Sprachen" auf die Option **Mails blockieren, die folgende Sprachen (Zeichensätze) verwenden** um E-Mails zu blockieren, die Zeichensätze verwenden, die für empfangene E-Mails untypisch sind, beispielsweise Chinesisch oder Vietnamesisch.

HINWEIS: Diese Funktion unterscheidet nicht zwischen Sprachen, die den gleichen Zeichensatz verwenden, beispielsweise Italienisch und Französisch.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.12 Keyword-Prüfung

Keyword-Prüfung erlaubt die Identifizierung von Spam-Mails mit Keywords in den empfangenen E-Mails.

Dieser Filter ist standardmäßig NICHT aktiviert.

Konfiguration der Keyword-Prüfung

1. Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► Keyword-Prüfung ► Eigenschaften**.

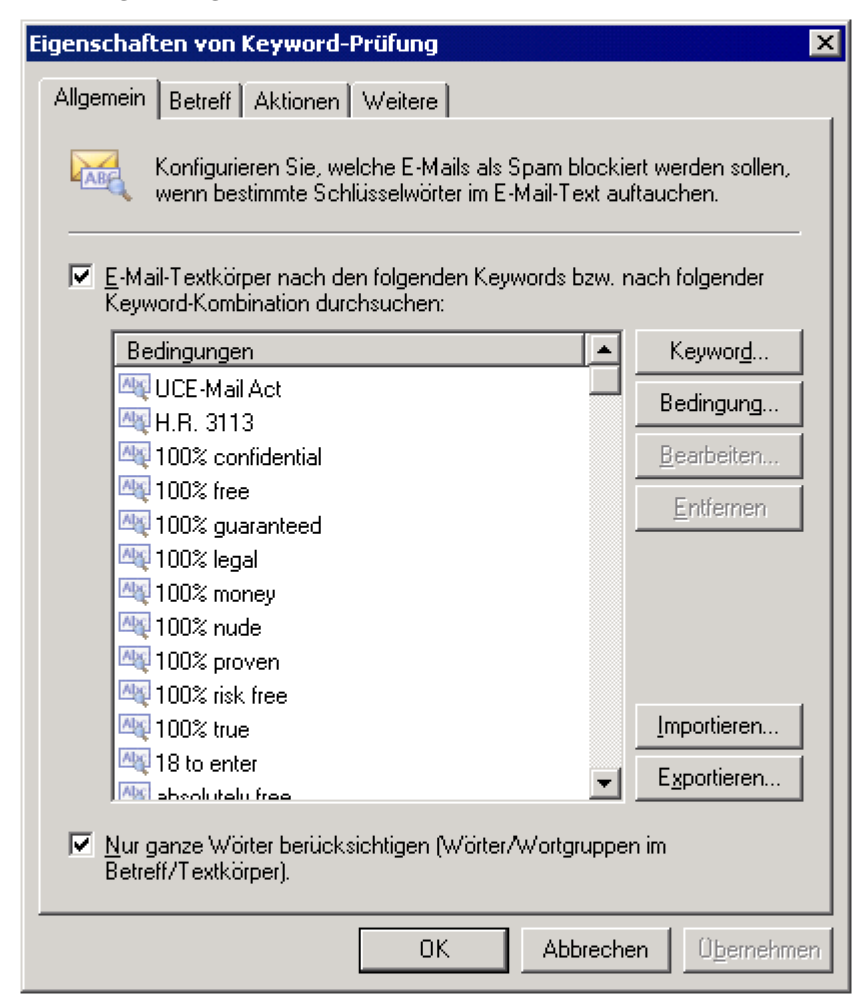


Bild 51 - Anti-Spam-Keyword-Prüfungseigenschaften

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Nachrichtentext auf folgende Keywords oder Keyword-Kombinationen scannen:** um diese Funktion zu aktivieren.

3. Klicken Sie auf die Schaltfläche **Keyword** um Keywords einzugeben. Wenn Sie mehrere Wörter eingeben, interpretiert GFI MailEssentials diese als Phrase.

- **Beispiel:** Bei Eingabe von 'Basketball Sport' sucht GFI MailEssentials nach der Phrase 'Basketball Sport'. Die Regel würde nur aktiviert, wenn diese Phrase gefunden wird, nicht, wenn nur das Wort Basketball oder Sport gefunden wird, aber dazwischen noch weitere Wörter stehen.

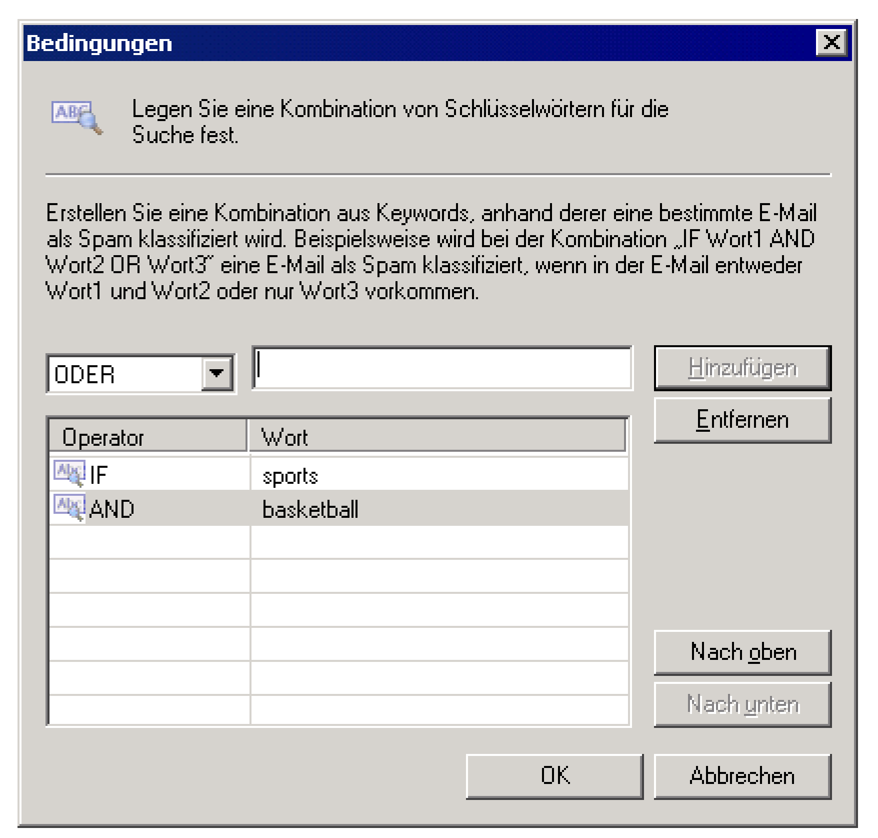


Bild 52 - Hinzufügen einer Bedingung

4. Ergänzen Sie logische Operatoren, indem Sie auf die Schaltfläche **Bedingungen …** klicken.

HINWEIS: Bedingungen sind Kombinationen von Keywords mit den Operanden IF, AND, AND NOT, OR oder OR NOT. Definieren Sie mit Bedingungen Wortkombinationen, die in der E-Mail vorkommen müssen.

- **Beispiel:** Eine Bedingung 'IF Wort1 AND Wort2' prüft, ob Wort1 und Wort2 vorkommen. Beide Wörter müssen in einer E-Mail gefunden sein, damit die betreffende Regel aktiviert wird.

Klicken Sie zum Hinzufügen einer Bedingung auf die Schaltfläche **Bedingungen …**

5. Wählen Sie die Registerkarte Betreff aus und aktivieren Sie das Kontrollkästchen **Die E-Mail-Betreffzeile auf die folgenden Keywords oder Kombinationen von Keywords scannen**. Konfigurieren Sie die Wörter, nach denen in der Betreffzeile der Nachricht gesucht werden soll.

- Klicken Sie zur Eingabe von Einzelwörtern oder Phrasen ohne logische Operatoren auf die Schaltfläche **Keyword …**
- Klicken Sie zur Eingabe von Keywords mit logischen Operatoren auf die Schaltfläche **Bedingungen …**

6. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

7. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

4.2.13 Neue Absender

Der Filter "Neue Absender" erlaubt es GFI MailEssentials automatisch E-Mails von Absendern zu identifizieren, an die noch nie E-Mails gesendet wurden. Solche Absender werden durch Vergleich mit den in der Whitelist erfassten Daten identifiziert.

NUR E-Mails, in denen keine Spam-Nachrichten erkannt wurden, und deren Absender nicht in der Whitelist eingetragen sind, werden in den Ordner Neue Absender übertragen.

Da solche E-Mails auch von berechtigten Benutzern stammen können, werden sie in einem speziellen Ordner gesammelt. Auf diese Weise können die E-Mails einfach identifiziert werden. Danach können Sie diese E-Mails prüfen und nicht erkannte Spam-Nachrichten in die benutzerdefinierten Blacklist eintragen.

Dieser Filter ist standardmäßig NICHT aktiviert.

Wichtige Hinweise

1. Aktivieren Sie mindestens eine der verfügbaren Whitelists um die Funktion Neue Absender zu verwenden. Wenn keine Whitelist zur Verfügung steht (wenn keine Spam durch andere Filter erkannt wurde), werden die empfangenen Nachrichten in das Empfängerpostfach übertragen. **NUR** E-Mails, in denen keine Spam-Nachrichten erkannt wurden, und deren Absender nicht in der Whitelist eingetragen sind, werden in den Ordner Neue Absender übertragen.

Konfiguration des Filters "Neue Absender"

1. Klicken Sie auf **Anti-Spam ► Neue Absender ► Eigenschaften**.

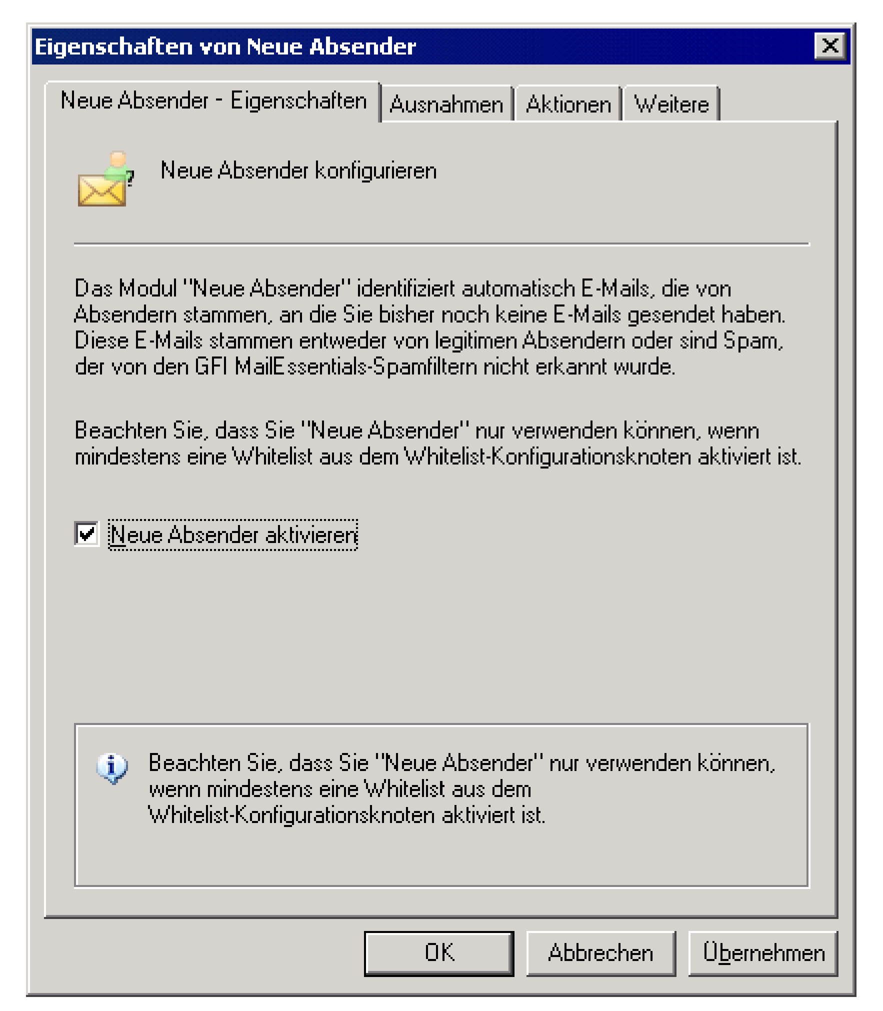


Bild 53 - Neue Absender - Eigenschaften

2. Klicken Sie auf der Registerkarte **Neue Absender - Eigenschaften** in das Kontrollkästchen **Neue Absender aktivieren** um die Prüfung aller eingehenden Nachrichten auf neue Absender zu aktivieren und klicken Sie auf **Übernehmen**.

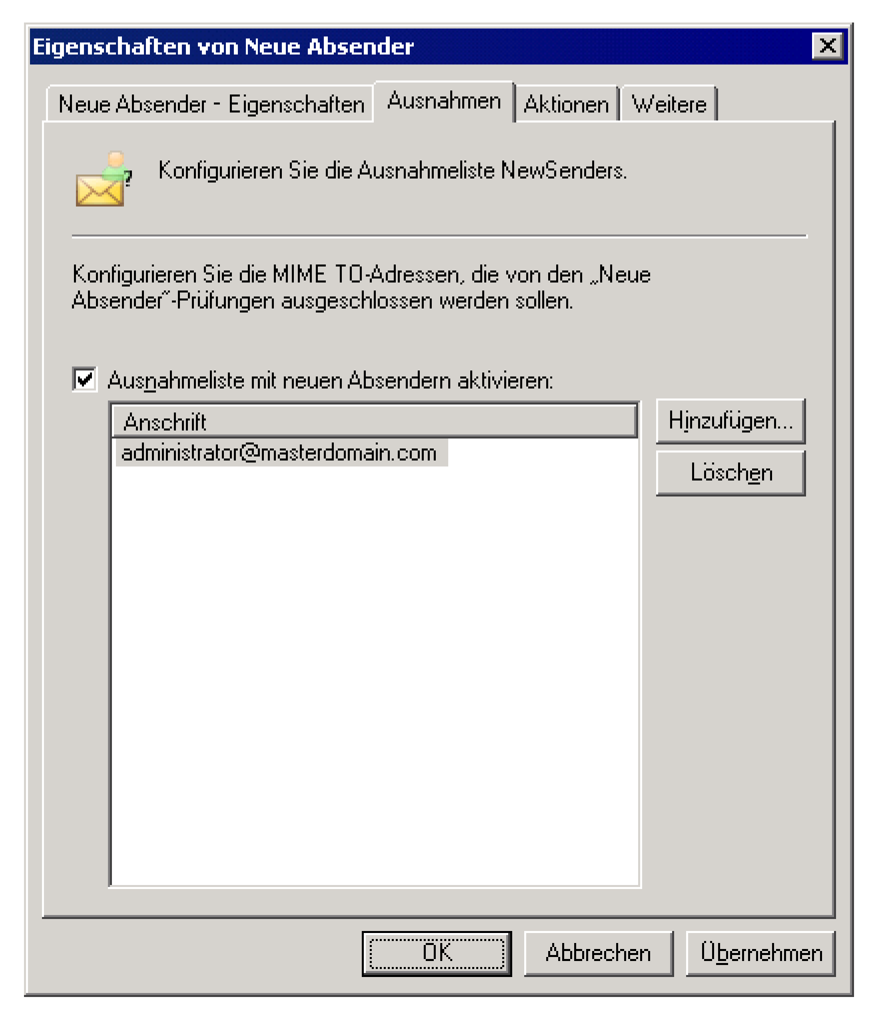


Bild 54 - Neue Absender-Ausnahmenkonfiguration

3. Klicken Sie auf die Registerkarte **Ausnahmen** und aktivieren Sie das Kontrollkästchen **MIME TO Ausnahmeliste:** um die lokalen Empfänger zu konfigurieren, deren E-Mails bei der Prüfung auf neue Absender ausgeschlossen werden sollen.

4. Klicken Sie auf die Schaltfläche **Hinzufügen …** und geben Sie die E-Mail-Adresse des Absenders ein.

- **Beispiel:** administrator@master-domain.com.

Wiederholen Sie dies für jede Adresse, die Sie hinzufügen wollen, und klicken Sie zum Speichern auf die Schaltfläche **Übernehmen**.

HINWEIS: Um Ihre Ausnahmeliste vorübergehend zu deaktivieren, müssen Sie nicht alle eingetragenen Adressen löschen, sondern brauchen nur das Kontrollkästchen **MIME TO Ausnahmeliste:** zu deaktivieren.

5. Klicken Sie auf die Registerkarte **Aktionen** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration abzuschließen.

4.2.14 Spam-Aktionen - Umgang mit Spam-Mails

Die Registerkarten **Aktionen** und **Weitere** in den Spam-Filterdialogen legen fest, wie mit als Spam identifizierten E-Mails verfahren werden soll. Für jeden einzelnen Spam-Filter können Sie andere Aktionen definieren. Auf diese Weise können Sie zum Speichern der erkannten Spam-Nachrichten für jeden Filter andere Ordner einrichten. Und Sie können sofort erkennen, warum eine E-Mail als Spam markiert wurde und die von einem bestimmten Filter blockierten E-Mails leichter verarbeiten.

- **Beispiel:** Löschen Sie E-Mails, die durch den Blacklist-Spam-Filter gekennzeichnet wurden, nicht aber E-Mails, die durch die Keyword-Prüfung als Spam markiert wurden.

HINWEIS: Die Optionen auf der Registerkarte Aktionen sind bei jedem Spam-Filter mit Ausnahme der Whitelist (Umgehung der Spam-Filter) und der Option "Neue Absender" (Spam kann dabei nicht in den Junk-Ordner verschoben werden) identisch.

Konfiguration von Spam-Aktionen

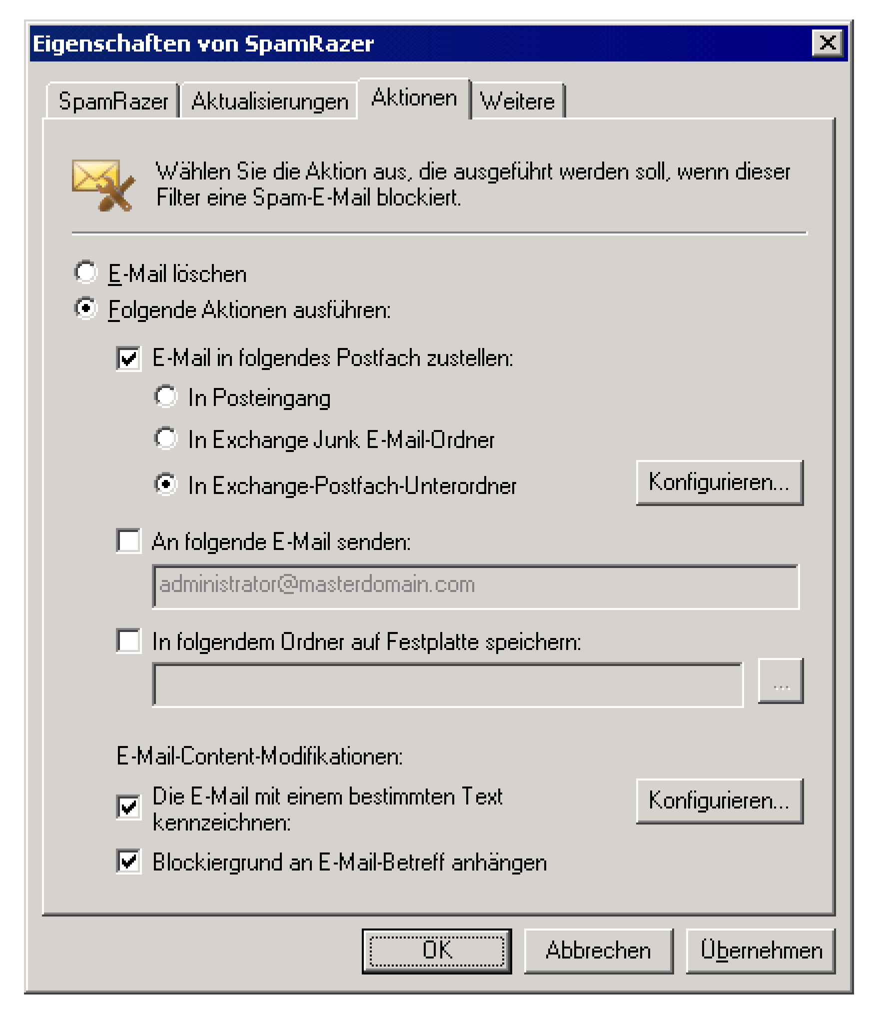


Bild 55 - Konfiguration der gewünschten Aktion

1. Klicken Sie auf der Registerkarte **Aktionen** auf eine Option, die festlegt, welche Aktion bei als Spam markierten E-Mails durchgeführt werden soll:

- **E-Mail löschen** - Löscht eine E-Mail, die durch einen bestimmten Spamfilter geblockt ist. Andere Spamoptionen werden deaktiviert, sobald die E-Mail gelöscht ist.
- **E-Mail in Postfach verschieben** - Wählen Sie den Ordner aus, in dem die E-Mail gespeichert werden soll:
  - **Im Posteingang** - Mit dieser Option leiten Sie die Spam-Mails in den Posteingang des Benutzers.
  - **In Exchange-Junk-Ordner des Benutzers verschieben** - Mit dieser Option verschieben Sie alle Spam-Mails in den Standard-Junk-Ordner des Benutzers.
  - **In den Postfach-Unterordner von Microsoft Exchange -** Mit dieser Option leiten Sie alle Spams in einen bestimmten Ordner des Benutzerpostfachs um. Klicken Sie auf **Konfigurieren**, um den Dialog "In Exchange-Ordner verschieben" zu starten und geben Sie den Ordner ein, in den die Spam-E-Mails verschoben werden sollen.
    - **Beispiel 1:** Geben Sie **vermutliche Spam** für einen benutzerdefinierten Ordner ein, der auf der gleichen Ebene wie der Posteingangsordner erstellt werden soll.
    - **Beispiel 2:** Geben Sie **Posteingang\vermutliche Spam** für einen benutzerdefinierten Ordner ein, der im Eingangspostfach erstellt werden soll.

    HINWEIS 1: Für diese Option müssen folgende Bedingungen erfüllt sein:

    - GFI MailEssentials muss auf einem Computer mit Microsoft Exchange Server installiert sein. Ist GFI MailEssentials nicht auf einem Microsoft Exchange Server installiert, verfahren Sie entsprechend dem Kapitel Verschieben von Spam-E-Mails in den Postfachordner des Benutzers Auf Seite 127 in diesem Handbuch
    - Die Active Directory muss aktiviert sein.
    - Es muss Microsoft Exchange Server 2000/2003 bzw. Microsoft Exchange Server 2007/2010 mit der Mailbox-Serverrolle vorhanden sein.

    HINWEIS 2: Damit diese Option aktiviert werden kann, ist bei Microsoft Exchange 2010 ein dezidierter Benutzer erforderlich. Klicken Sie im Dialog Aktionen auf **Konfigurieren** und dann auf **Benutzerkonto festlegen**, um den dezidierten Benutzer zu definieren. Wählen Sie im Konfigurationsdialog In Exchange verschieben eine der folgenden Optionen aus:

    - **Spam mit automatisch erstelltem Benutzer verschieben** - Wählen Sie diese Option aus, damit GFI MailEssentials automatisch einen Benutzer mit allen erforderlichen Rechten einrichten kann.
    - **Spam in folgendes Benutzerkonto verschieben** - Wählen Sie diese Option aus, um einen manuell erstellten Benutzer zu verwenden. Geben Sie die Anmeldedaten (Domäne\Benutzername und Kennwort) eines dezidierten Benutzers an und klicken Sie auf **Zugriffsrechte**

definieren, um dem angegebenen Benutzer die erforderlichen Rechte zuzuweisen.

HINWEIS: Die manuell angegebenen Benutzeranmeldedaten dürfen nur für diese Funktion gelten. Benutzername, Kennwort und sonstige Eigenschaften dürfen NICHT von Microsoft Exchange oder Active Directory abweichen, sonst funktioniert die Funktion zum Verschieben in den Exchange-Ordner nicht.

- **An E-Mail-Adresse weiterleiten** - Die als Spam gekennzeichnete E-Mail wird an eine spezifische E-Mail-Adresse weitergeleitet.
  - **Beispiel:** Eine E-Mail-Adresse eines öffentlichen Ordners. Auf diese Weise kann jemand beauftragt werden, regelmäßig die als Spam gekennzeichneten E-Mails zu überprüfen und E-Mails zu identifizieren, die fälschlicherweise als Spam gekennzeichnet wurden. Mit dieser Funktion lässt sich außerdem der Spam-Filter verfeinern.

  Der Betreff der E-Mail hat das Format **[recipient] [subject]**
- **In definierten Ordner auf Festplatte speichern** - Speichert alle als Spam markierten E-Mails unter dem angegebenen Pfad.
  - **Beispiel:** 'C:\Spam\'.

  Der Dateiname der gespeicherten E-Mail hat folgendes Format:

  `[Sender_recipient_subject_number_.eml]` (Beispiel: `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)
- **E-Mail mit bestimmtem Text markieren** - Mit dieser Option ergänzen Sie einen Text in der E-Mail-Betreffzeile. Klicken Sie auf **Konfigurieren**, um die Kennzeichnungsoptionen zu ändern. Geben Sie in dem Dialog "E-Mail kennzeichnen" den Text ein, den Sie für die Kennzeichnung verwenden wollen und geben Sie an, wo die Kennzeichnung platziert werden soll:
  - **Vor Betreff einfügen** - Die angegebene Kennzeichnung wird am Anfang eingefügt, das heißt als Präfix, vor dem Betreff der E-Mail.
    - **Beispiel:** '[SPAM] Kostenlose Web-Mail-Adresse'.
  - **An Betreff anhängen** - Die definierte Kennzeichnung wird am Ende, das heißt als Suffix, am Text der Betreffzeile angehängt.
    - **Beispiel:** 'Kostenlose Web-Mail-Adresse (Spam])'.
  - **Kennzeichnung in neuem X-Header hinzufügen...** - Die definierte Kennzeichnung wird als neuer X-Header in der E-Mail eingefügt. In diesem Fall hat der X-Header folgendes Format:

    `X-GFIME-SPAM: [TAG TEXT]`

    `X-GFIME-SPAM-REASON: [GRUND]`

    - **Beispiel:**

    `X-GFIME-SPAM: [Das ist SPAM]`

    `X-GFIME-SPAM-REASON: [DNSBL Prüfung fehlgeschlagen - Versand über Blacklist-Domäne]`

- **Grund für die Blockierung an E-Mail-Betreff anhängen -** Wenn Sie diese Option auswählen, werden der Name des Filters, der die E-Mail blockiert hat und der Grund für die Blockierung in der Betreffzeile der blockierten E-Mail angehängt.

Weitere Optionen

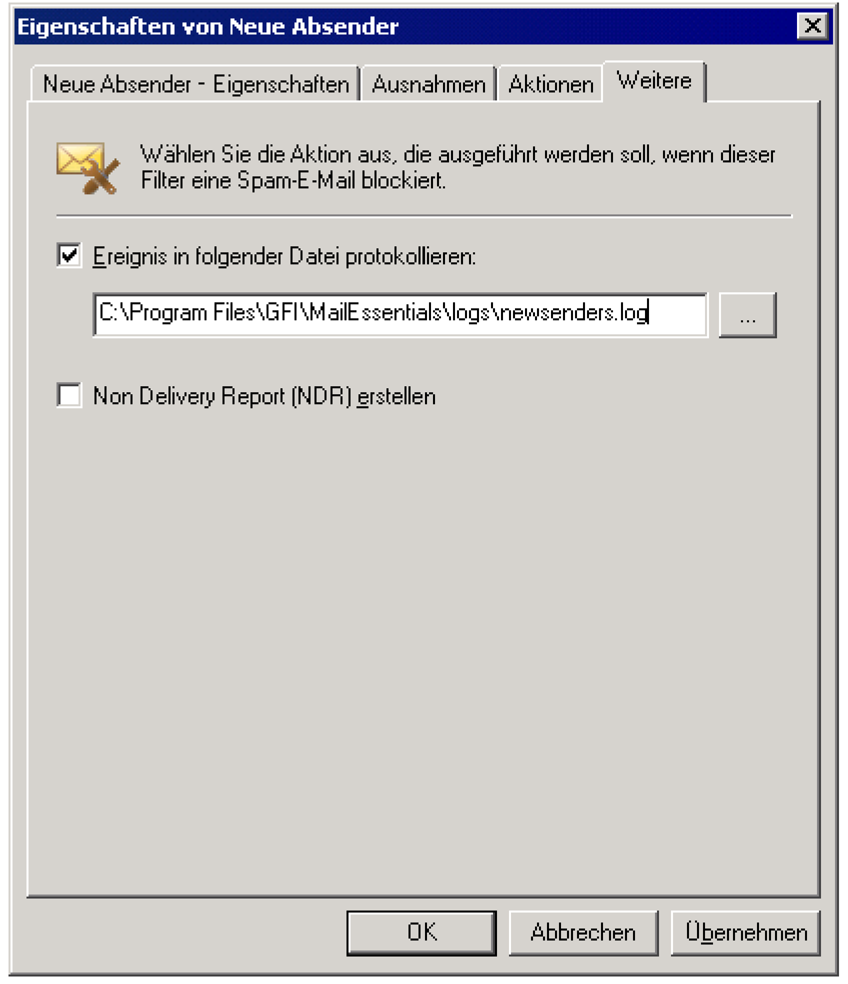


Bild 56 - Registerkarte "Weitere Aktionen"

Klicken Sie auf die Registerkarte **Weitere** um eine Reihe von Zusatzaktionen zu definieren:

- **Häufigkeit in dieser Datei protokollieren** - Protokollieren Sie die Häufigkeit der Spam-Mail in einer von Ihnen definierten Protokolldatei.
- **Unzustellbarkeitsbericht (NDR) erzeugen** - Erstellt und versendet einen Pseudo-Unzustellbarkeitsbericht (NDR). Bei Erhalt eines NDR entfernt Massen-Mailer-Software Ihre Adresse aus der jeweiligen Datenbank. Diese Option können Sie auch nutzen, um den Absender zu informieren, dass die E-Mail als Spam betrachtet wurde.

HINWEIS: Um den Pseudo-Unzustellbarkeitsbericht "ndr.xml" anzupassen, bearbeiten Sie ihn in dem Verzeichnis MailEssentials\templates mit Notepad oder einem XML-Editor.

4.2.15 Globale Spam-Aktionen

Viel Spam wird an E-Mail-Adressen versendet, die nicht mehr existieren. Allgemein werden diese E-Mails einfach gelöscht, zur Problembehandlung oder für Testzwecke können Sie diese E-Mails jedoch in einen Ordner verschieben oder an eine bestimmte E-Mail-Adresse weiterleiten.

HINWEIS: Dieser Abschnitt bezieht sich nur auf Installationen von Microsoft Exchange Server, bei denen die Funktion **In Spam-Ordner des Benutzers weiterleiten** aktiviert ist. Bei anderen Servern wird die Registerkarte "Globale Spam-Aktionen" nicht angezeigt.

Konfiguration der globalen Spam-Aktionen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam ► Anti-Spam-Einstellungen** und dann auf **Eigenschaften**.

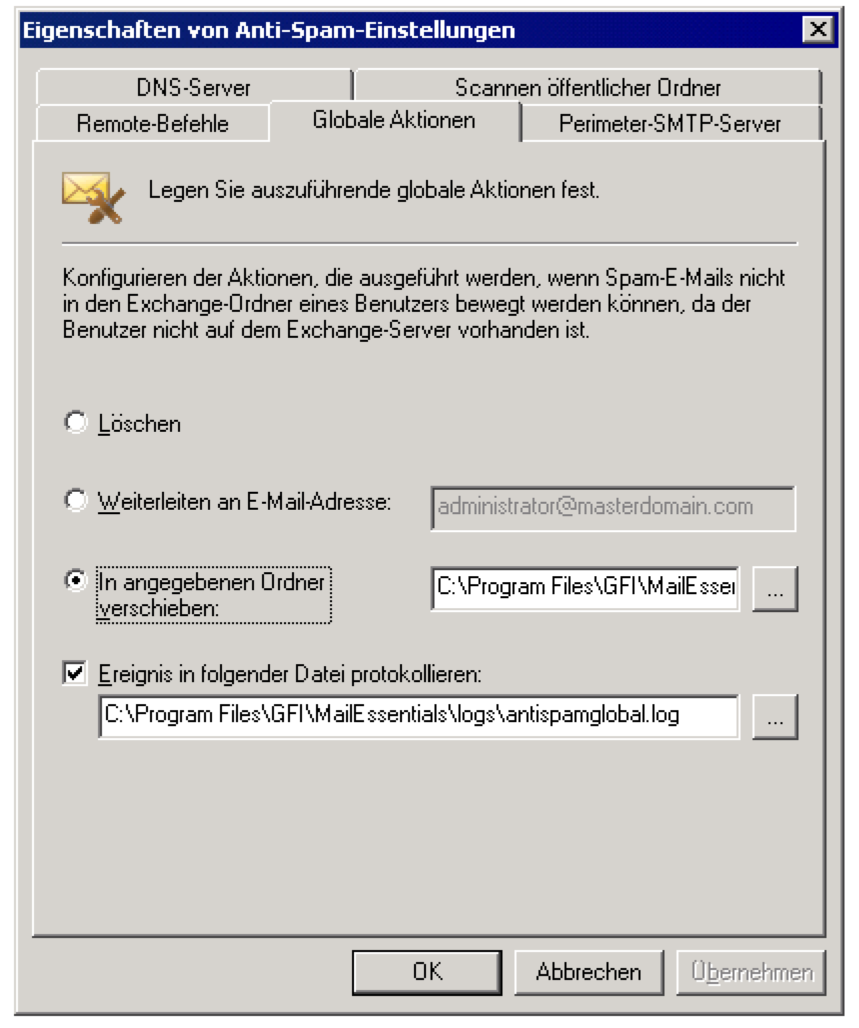


Bild 57 - Globale Aktionen

2. Klicken Sie auf die Registerkarte **Globale Aktionen** und wählen Sie eine der folgenden Optionen aus:

- E-Mail löschen
- E-Mail an eine bestimmte E-Mail-Adresse weiterleiten
- E-Mail in einen definierten Ordner verschieben

3. Klicken Sie auf **Häufigkeit in dieser Datei protokollieren** um eine Spam-Mail in einer Protokolldatei zu erfassen.

4.2.16 Sortieren von Spam-Filtern nach Priorität

In GFI MailEssentials können Sie die Reihenfolge festlegen, in der Spam-Prüfungen für eingehende Nachrichten ausgeführt werden.

HINWEIS: Die Reihenfolge aller verfügbaren Filter können Sie anpassen. Nur der Neue Absender hat automatisch immer die niedrigste Priorität. Dies hängt damit zusammen, dass zuvor die Ergebnisse der Whitelist sowie der anderen Spam-Filter geprüft werden müssen.

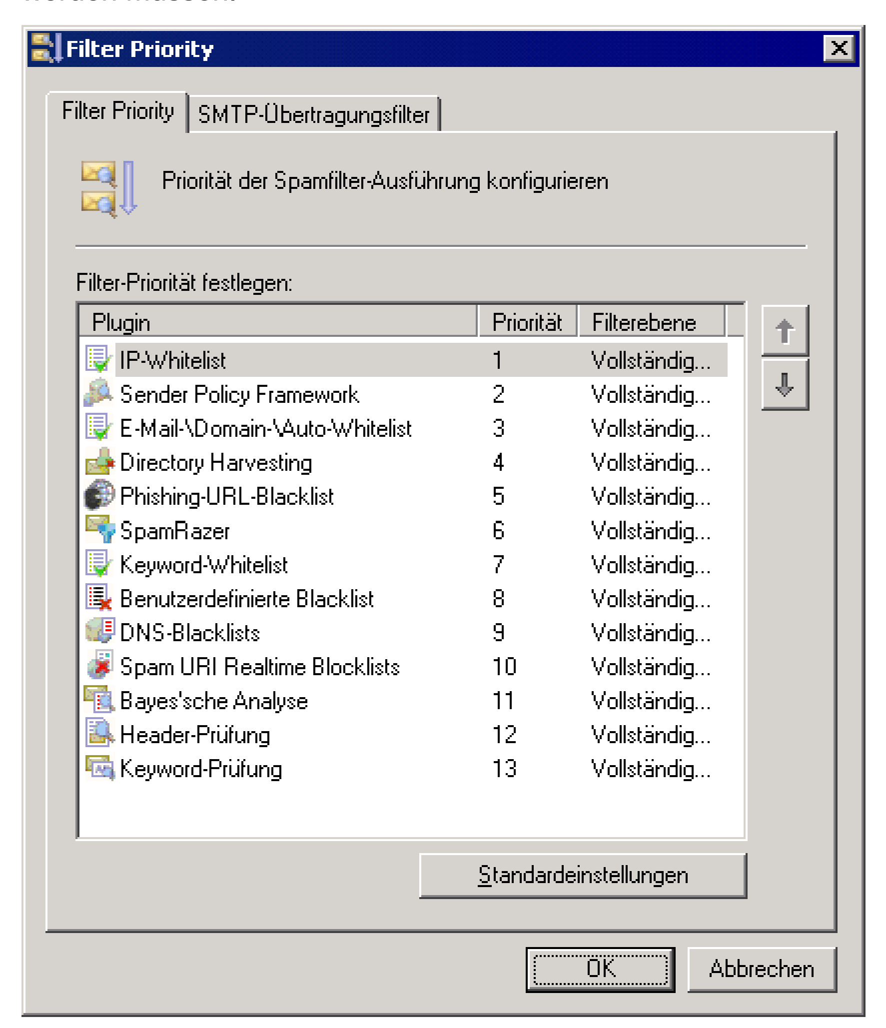


Bild 58 - Zuordnung von Filterprioritäten

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam ► Filterpriorität** und dann auf **Eigenschaften**.

2. Klicken Sie auf einen Filter und dann auf die Schaltfläche <Aufwärts> um den ausgewählten Filter eine höhere Priorität zuzuordnen oder auf die Schaltfläche <Abwärts> um dem ausgewählten Filter eine niedrigere Priorität zu geben.

HINWEIS: Klicken Sie auf die Schaltfläche **Standardeinstellungen** um die Filterreihenfolge wieder auf den Standard einzustellen.

3. Klicken Sie auf die Schaltfläche **OK** um die Konfiguration zu übernehmen. Die Änderungen werden sofort wirksam.

4.3 Haftungsausschluss

Haftungsausschlüsse sind Standardtexte, die am Beginn oder am Ende ausgehender E-Mails aus juristischen oder Marketinggründen eingefügt werden. Sie helfen den Unternehmen, sich gegen Klagen zu schützen, die mit dem Inhalt einer E-Mail zusammenhängen, und ergänzen Beschreibungen über die angebotenen Produkte und Dienstleistungen.

Wichtige Hinweise

1. Haftungsausschlüsse werden nur bei ausgehenden E-Mails ergänzt.

2. Starten Sie die IIS-Dienste und GFI MailEssentials neu, nachdem Sie einen Haftungsausschluss deaktiviert haben, damit die Änderungen wirksam werden.

4.3.1 Konfiguration von Haftungsausschlüssen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **E-Mail-Verwaltung ► Haftungsausschluss** und dann auf **Neu ► Haftungsausschluss**.

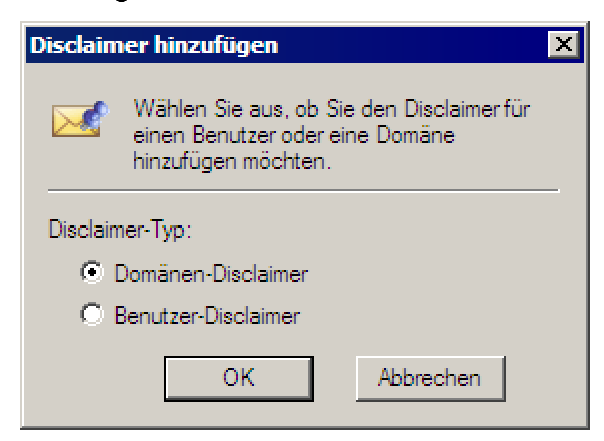


Bild 59 - Auswahl eines Haftungsausschlusses für eine Domäne oder einen Benutzer

2. Wählen Sie:

- **Domäne** - Wählen Sie die Domäne aus der Liste der konfigurierten Domäne. Alle von dieser Domäne versendeten E-Mails enthalten den ergänzten Haftungsausschluss
- **Benutzer** - Geben Sie an, bei welchem Benutzer oder bei welcher Benutzergruppe der Haftungsausschluss bei ausgehenden E-Mails ergänzt werden soll. Wenn GFI MailEssentials im Active Directory-Modus arbeitet, entnehmen Sie die Benutzer bzw. die Benutzergruppen direkt aus der Active Directory; anderenfalls geben Sie die SMTP-E-Mail-Adresse des Benutzers an.

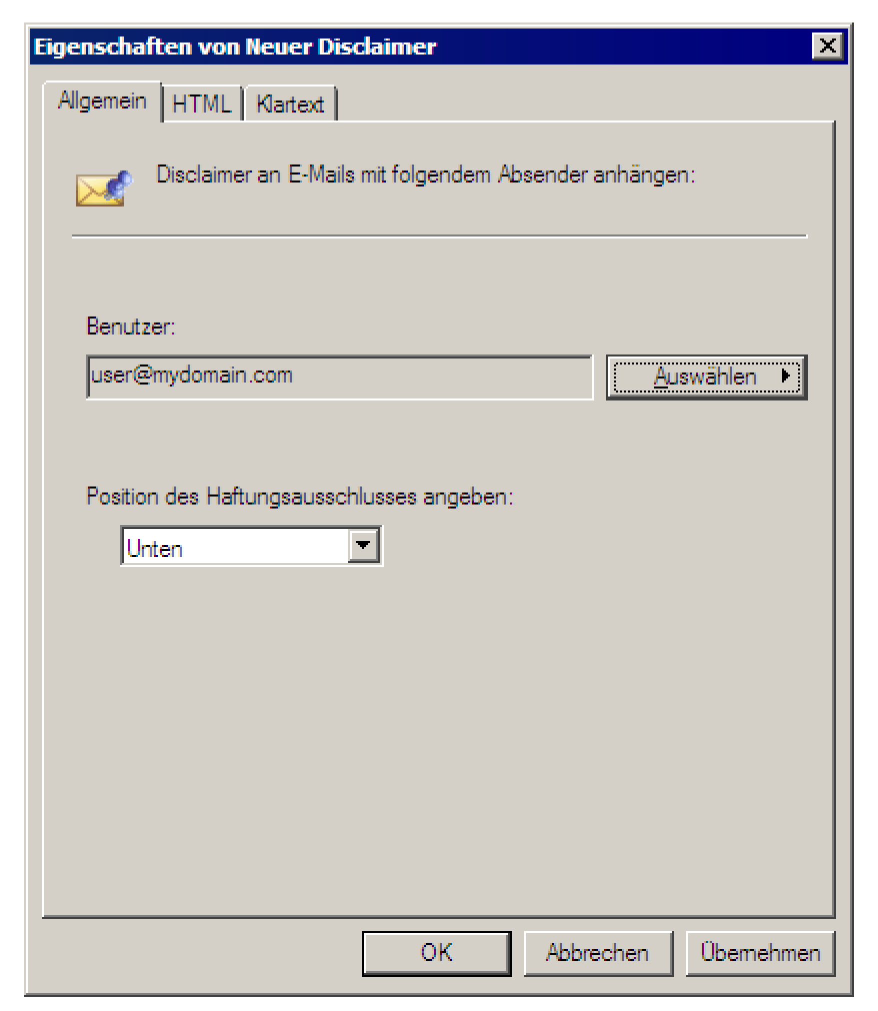


Bild 60 - Neuer Haftungsausschluss - Allgemeine Eigenschaften

3. Klicken Sie in der Registerkarte **Allgemein** auf **Auswählen**, um die Domäne oder den Benutzer zu ändern. Klicken Sie auf **oben** oder **unten,** um festzulegen, ob der Haftungsausschluss am Anfang oder Ende der E-Mail eingefügt werden soll.

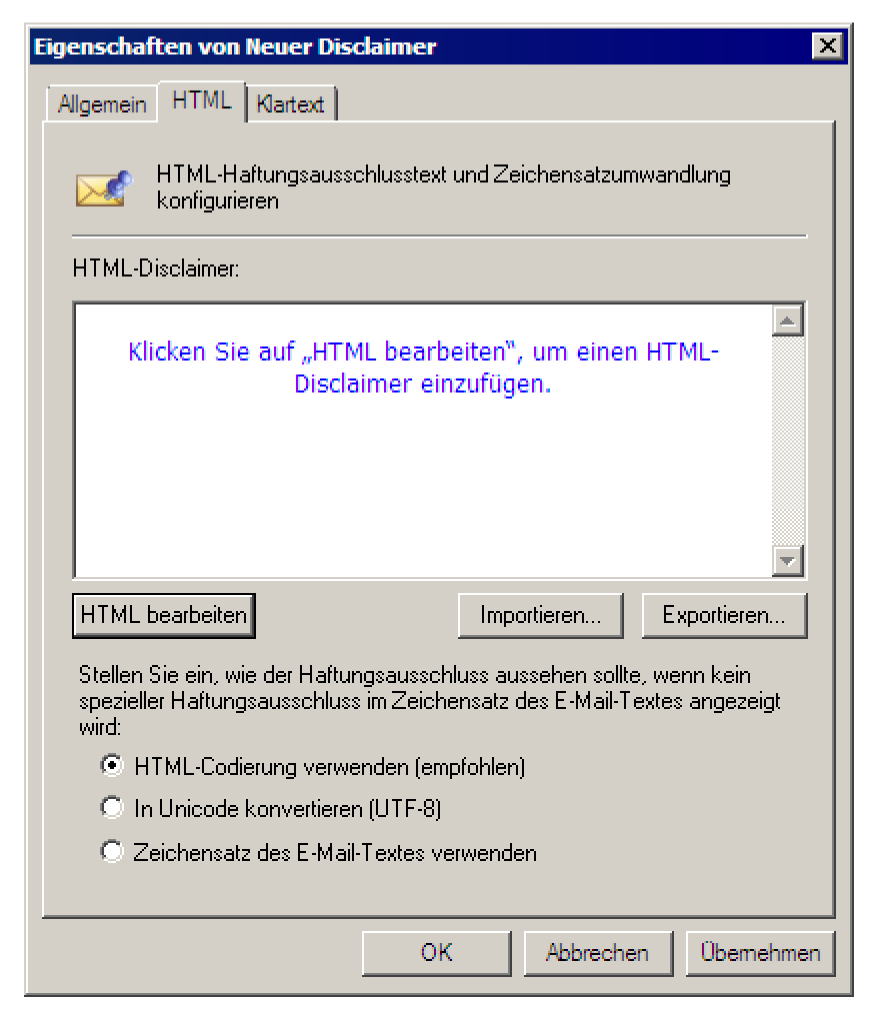


Bild 61 - HTML-Haftungsausschluss

4. Klicken Sie zum Hinzufügen eines Haftungsausschlusses im 'HTML-Format' auf die Registerkarte HTML. Klicken Sie auf **HTML bearbeiten**, um den Editor für den HTML-Haftungsausschluss zu öffnen und den Text für den HTML-Haftungsausschluss zu bearbeiten.

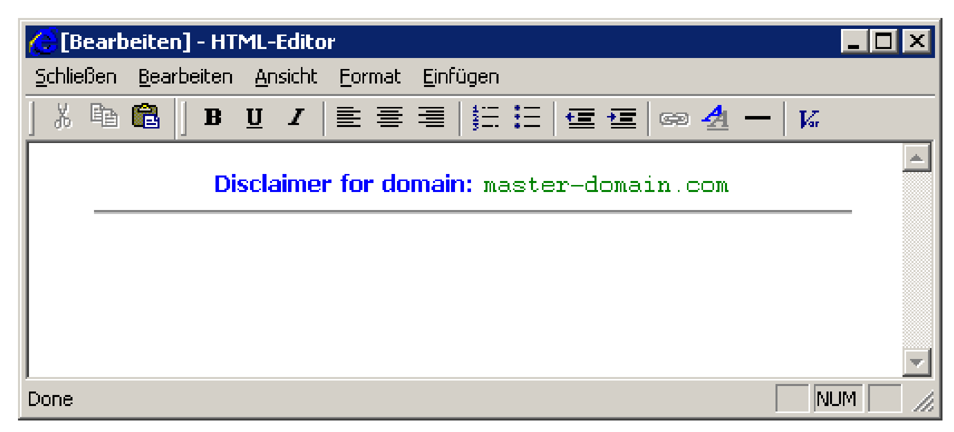


Bild 62 - HTML-Editor für den Haftungsausschluss

HINWEIS 1: Für HTML-Haftungsausschlüsse benutzen Sie den Editor wie eine einfache Textverarbeitung. Variablen fügen Sie mit der Menü-Option **Einfügen** ein. Variablen werden in der E-Mail durch den tatsächlichen Namen des Empfängers oder Senders ersetzt. Fügen Sie folgende Felder in den Haftungsausschluss ein:

- [Datum]
- [Absendername]
- [Absender-E-Mail]
- [Empfängername]
- [Empfänger-E-Mail]

HINWEIS 2: Die Variablen für den angezeigten Namen des Empfängers und seine E-Mail-Adresse werden nur ersetzt, wenn die E-Mail an einen einzigen Empfänger versendet wird. Wenn E-Mails an mehrere Empfänger versendet werden, werden die Variablen durch 'Empfänger' ersetzt.

5. Klicken Sie auf **Schließen**, um den HTML-Haftungsausschluss hinzuzufügen.

6. Geben Sie die Codierung für den HTML-Haftungsausschluss an, wenn der Zeichensatz für den E-Mail-Text nicht HTML ist:

- **HTML-Codierung verwenden** - definieren Sie mit der HTML-Codierung die Zeichensätze für den E-Mail-Text und den Haftungsausschluss. Diese Option wird empfohlen.
- **In Unicode konvertieren** - konvertiert den E-Mail-Text und den Haftungsausschluss in Unicode, so dass beide Teile richtig angezeigt werden.
- **Zeichensatz des E-Mail-Textes verwenden** - der Haftungsausschluss wird in den Zeichensatz des E-Mail-Textes konvertiert.

  Hinweis: Ist diese Option ausgewählt, wird eventuell nicht der ganze Text des Haftungsausschlusses richtig angezeigt.

7. Importieren oder exportieren Sie einen HTML-Haftungsausschluss mit den Schaltflächen **Importieren** bzw. **Exportieren**.

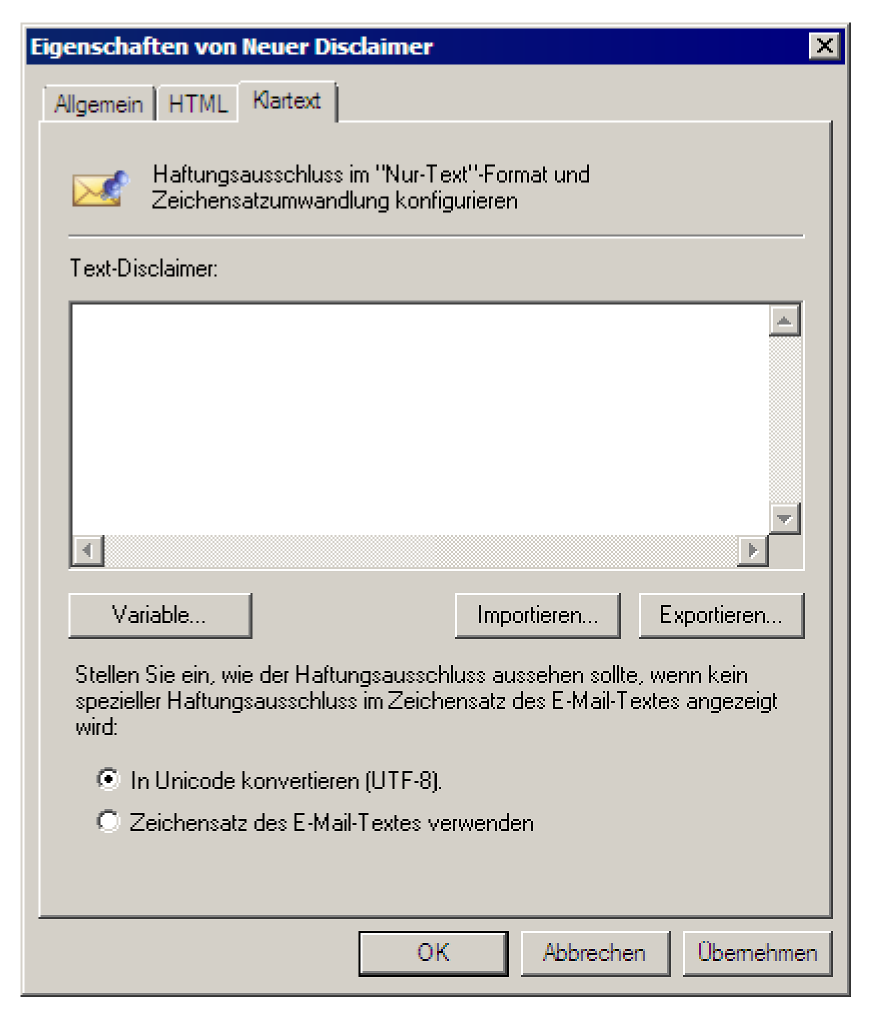


Bild 63 - 'Nur-Text'-Haftungsausschluss

8. Eine Textversion Ihres Haftungsausschlusses kann auch in reinen Text-E-Mails eingefügt werden. Klicken Sie auf die Registerkarte **Nur-Text** und fügen Sie den Text direkt in das Feld **Text Haftungsausschluss** ein. Fügen Sie mit der Schaltfläche **Variable …** Variablen hinzu.

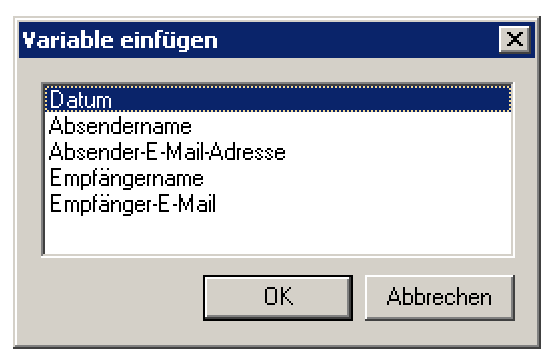


Bild 64 - Einfügen von Variablen in Ihren Haftungsausschluss

HINWEIS: Die Variablen für den angezeigten Namen des Empfängers und seine E-Mail-Adresse werden nur ersetzt, wenn die E-Mail an einen einzigen Empfänger versendet wird. Wenn E-Mails an mehrere Empfänger versendet werden, werden die Variablen durch 'Empfänger' ersetzt.

9. Geben Sie die Codierung für den Haftungsausschluss im 'Nur-Text'

Format an, wenn der Zeichensatz des E-Mail-Textes nicht das 'Nur-Text'-Format ist:

- **In Unicode konvertieren** - konvertiert E-Mail-Text und Haftungsausschluss in Unicode, so dass beide Teile richtig angezeigt werden.
- **Zeichensatz des E-Mail-Textes verwenden** - der Haftungsausschluss wird in den Zeichensatz des E-Mail-Textes konvertiert.

  Hinweis: Ist diese Option ausgewählt, wird eventuell nicht der ganze Text des Haftungsausschlusses richtig angezeigt.

10. Importieren oder exportieren Sie einen Haftungsausschluss im 'Nur-Text'-Format mit den Schaltflächen **Importieren** und **Exportieren**.

Der neu erstellte Haftungsausschluss wird auf der rechten Seite der Konfigurationskonsole von GFI MailEssentials angezeigt. Um dem neuen Haftungsausschluss einen aussagefähigen Namen zu geben, klicken Sie mit der rechten Maustaste auf den Haftungsausschluss und dann auf **Umbenennen**.

4.3.2 Aktivieren und Deaktivieren von Haftungsausschlüssen

Standardmäßig werden neue Haftungsausschlüsse automatisch aktiviert. So aktivieren oder deaktivieren Sie einen Haftungsausschluss:

1. Klicken Sie mit der rechten Maustaste auf den zu deaktivierenden Haftungsausschluss.

2. Klicken Sie auf **Deaktivieren** oder **Aktivieren** um die gewünschte Aktion auszuführen.

4.4 Automatische Antworten

Die Funktion "Automatische Antwort" erlaubt einen Versand automatischer Antworten an bestimmte eingehende E-Mails. Für jede E-Mail-Adresse bzw. Betreffzeile können Sie eine andere automatische Antwort definieren. Sie können in einer automatischen Antwort mit Variablen eine E-Mail personalisieren.

Wichtige Hinweise

1. Fügen Sie keinen Nachrichtentext ein, der mehr als 30 bis 40 Zeichen pro Zeile mit Zeilensprung enthält. Einige ältere E-Mail-Server schneiden Zeilen bei 30 bis 40 Zeichen ab.

4.4.1 Konfiguration von automatischen Antworten

1. Klicken Sie mit der rechten Maustaste auf den Knoten **E-Mail-Verwaltung ► Automatische Antwort** und dann auf **Neu ► Automatische Antwort**.

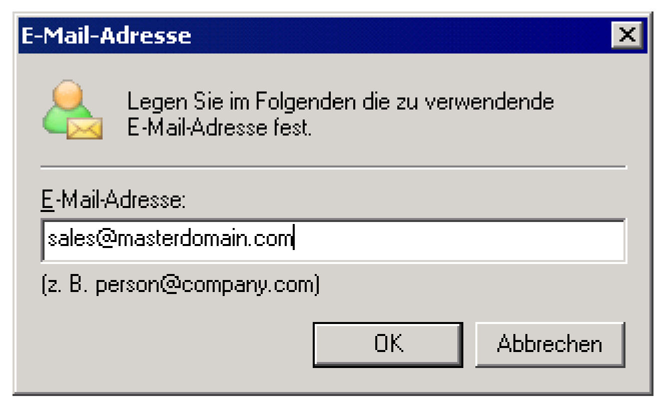


Bild 65 - Erstellen einer neuen automatischen Antwor

2. Geben Sie die E-Mail-Adresse ein, die Sie für die automatische Antwort konfigurieren wollen, und klicken Sie auf **OK**.

- **Beispiel** - Wenn Sie 'sales@master-Domäne.com' angeben, werden an diese E-Mail-Adresse gesendete E-Mails automatisch beantwortet.

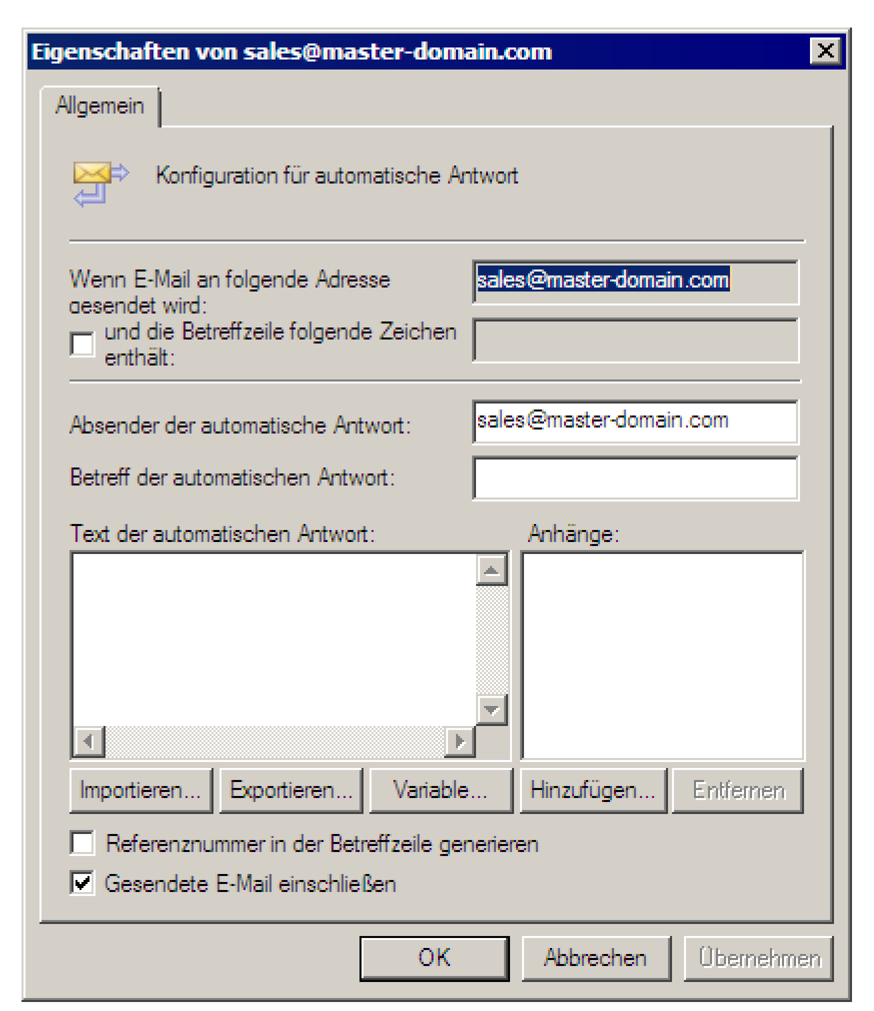


Bild 66 - Automatische Antwort - Eigenschaften

3. Aktivieren Sie das Kontrollkästchen **Betreff enthält** um automatische Antworten für E-Mails zu aktivieren, die in der Betreffzeile einen bestimmten Text enthalten.

4. Definieren Sie in dem Feld **Automatische Antwort von:** eine E-Mail-Adresse, wenn eine automatische Antwort von einer anderen E-Mail-Adresse als der E-Mail-Adresse erfolgen soll, an die die eingehende E-Mail gesendet wurde.

5. Geben Sie in dem Feld **Betreff automatische Antwort** den Betreff für die E-Mail mit der automatischen Antwort an.

6. Definieren Sie in dem Bearbeitungsfeld **Automatische Antwort - Text** den Text, der in der E-Mail mit der automatischen Antwort angezeigt werden soll.

HINWEIS: Importieren Sie den Text für die automatische Antwort aus einer Textdatei mit der Schaltfläche **Importieren ….**

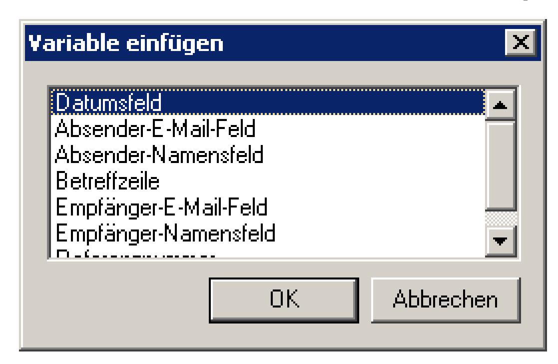


Bild 67 - Der Dialog "Variablen"

7. Klicken Sie auf **Variable…** um die automatischen Antworten mit Variablen zu personalisieren. Klicken Sie auf das Feld für die Variable um die Variable einzufügen und anschließend auf **OK**. Verfügbare Variablen sind:

1. **Datumsfeld** - setzt das Sendedatum der E-Mail ein.

2. **Absender-E-Mail-Feld** - setzt die E-Mail-Adresse des Absenders ein.

3. **Absender-Namensfeld** - setzt den angezeigten Namen des Absenders ein.

4. **Betreff-Feld** - setzt den Betreff für die E-Mail ein.

5. **Empfänger-E-Mail-Feld** - fügt die E-Mail-Adresse des Empfängers ein.

6. **Empfänger-Namensfeld** - fügt den angezeigten Namen des Empfängers ein.

7. **Referenznummer** - fügt Referenznummern ein (sofern erzeugt).

8. Klicken Sie auf **Hinzufügen...** und dann auf Dateianhänge, die mit der automatischen Antwort-E-Mail versendet werden sollen. Entfernen Sie Dateianhänge mit der Schaltfläche **Entfernen**.

9. Klicken Sie auf die Option **Gesendete E-Mail einfügen** um die eingegangene E-Mail in der automatischen Antwort zu zitieren.

10. Klicken Sie auf **Referenznummer in Betreffzeile erzeugen** um in den automatischen Antworten Referenznummern zu erzeugen.

HINWEIS: Mit dieser Funktion können Kunden beispielsweise eine Referenznummer angeben, mit der Mitarbeiter E-Mails besser zurückverfolgen können.

11. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

Standardmäßig werden Referenznummern in folgendem Format erzeugt:

- `ME_JJMMTT_nnnnnn`

Bedeutung:

- **ME -** GFI MailEssentials-Tag.
- **JJMMTT -** Datum im Format Jahr, Monat und Tag.
- **nnnnnn -** automatisch erzeugte Referenznummer.

4.5 Listenservers

Listenserver unterstützen die Erstellung von zwei Arten von Verteilerlisten:

1. Newsletter-Abonnenten-Liste - Genutzt wird diese Funktion zum Erstellen von Abonnementlisten für Firmen- oder Produkt-Newsletter, bei denen sich Benutzer eintragen oder austragen können.

2. Diskussionsliste - Mit dieser Option können Gruppen von Personen Diskussionen per E-Mail führen, wobei jedes Mitglied der Liste jede E-Mail empfängt, die ein Benutzer an die Liste sendet.

4.5.1 Erstellen eines Newsletters oder einer Diskussionsliste

1. Klicken Sie mit der rechten Maustaste in der Konfigurationskonsole von GFI MailEssentials auf **E-Mail-Verwaltung ► Listenserver** und anschließend auf **Neu ► Newsletter** oder **Diskussionsliste.**

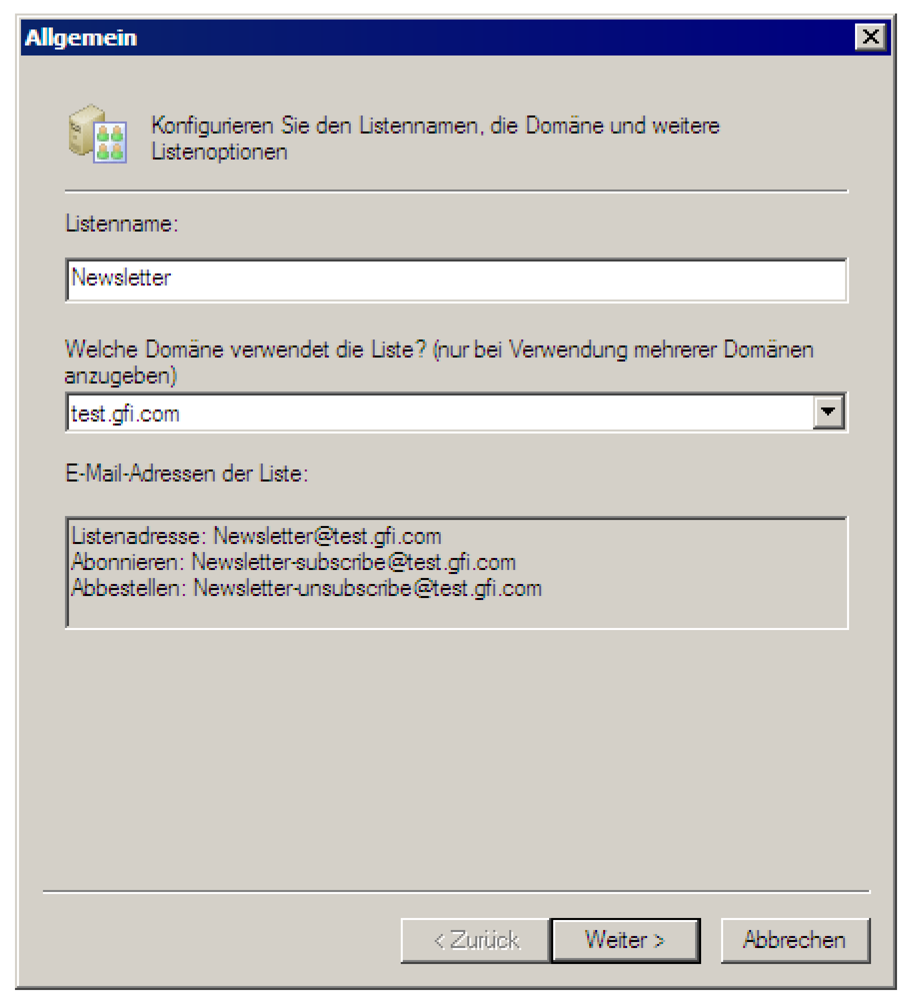


Bild 68 - Erstellen einer neuen Newsletter Newsletter-Liste

2. Geben Sie in dem Feld **Listenname:** einen Namen für die neue Liste ein und wählen Sie eine Domäne für die Liste aus (nur wenn Sie mehrere Domänen besitzen). Klicken Sie auf **Weiter** um fortzufahren.

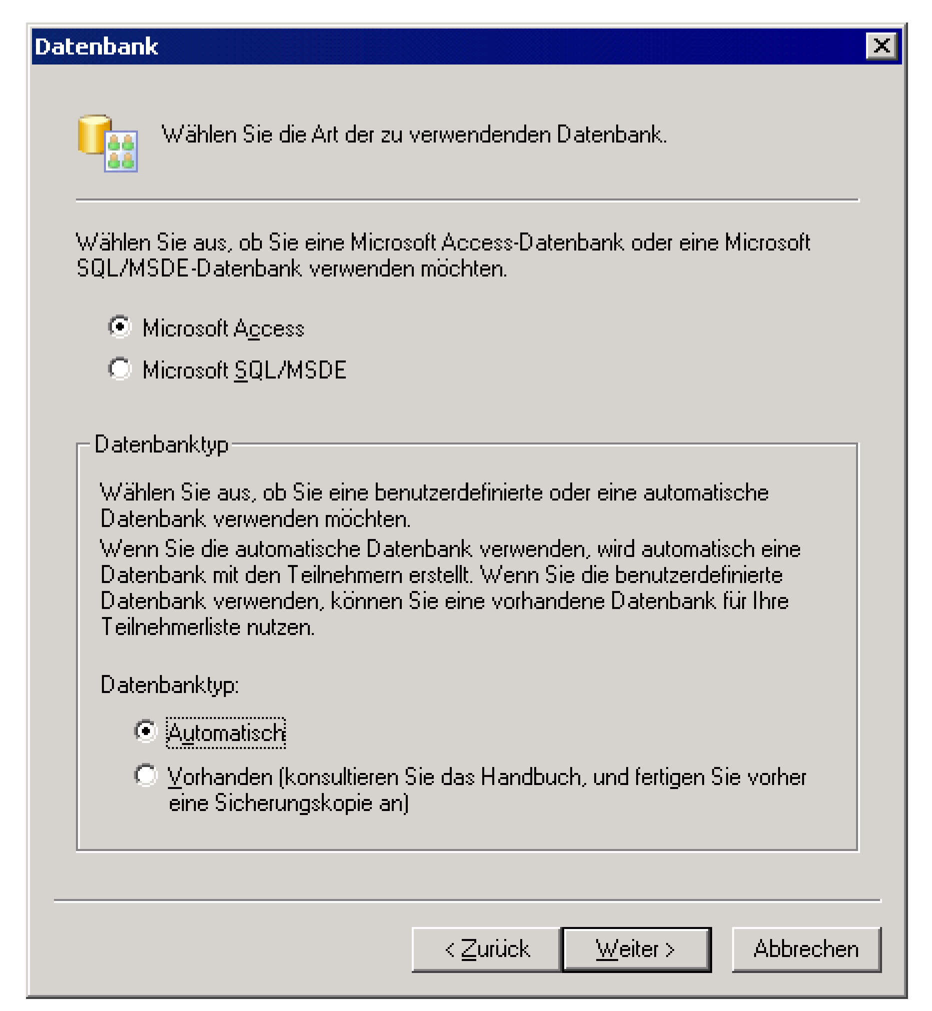


Bild 69 - Definition des Datenbank-Backends

3. Wählen Sie **Microsoft Access** oder **Microsoft SQL Server/MSDE** als Datenbank aus und in der Gruppe **Datenbanktyp**, ob GFI MailEssentials eine neue Datenbank erstellen oder eine Verbindung mit einer vorhandenen Datenbank aufbauen soll. Klicken Sie auf Weiterum fortzufahren.

HINWEIS 1: Für kleinere Listen mit bis zu 5.000 Mitgliedern können Sie Microsoft Access als Backend verwenden.

HINWEIS 2: Um eine neue Datenbank zu erstellen, klicken Sie auf die Option **Automatisch**.

4. Konfigurieren Sie den ausgewählten Datenbanktyp zur Speicherung der Newsletter-/Diskussions-Listen. Die verfügbaren Optionen sind:

Datenbanktyp	Datenbankeinstellungen
Microsoft Access mit der Option "Automatisch"	Geben Sie in dem Bearbeitungsfeld Datei an, wo die neue Datenbank gespeichert ist.
Microsoft Access mit der Option "Vorhanden"	Geben Sie in dem Feld Datei den Pfad zu Ihrer vorhandenen Microsoft Access-Datenbank ein, die die Newsletter-/Diskussionsabonnenten enthält. Klicken Sie in der Dropdown-Liste Tabelle auf die Tabelle, in der die Abonnentenliste gespeichert ist.
Microsoft SQL Server mit Option	Geben Sie den Namen des SQL-Servers, die Anmeldedaten und die Datenbank zur

"Automatisch"	Speicherung der Newsletter-/Diskussionsabonnentenliste an.
Microsoft SQL mit der Option "Vorhanden"	Geben Sie den Namen des SQL-Servers und die Anmeldedaten ein und wählen Sie die Datenbank und die Datentabelle, in der die Abonnenten gespeichert werden.

5. Klicken Sie bei allen Datenbanktypen mit der Option **Automatisch** zum Abschluss des Assistenten auf die Schaltfläche **Fertigstellen** oder auf die Schaltfläche **Weiter** um mit dem Setup fortzufahren.

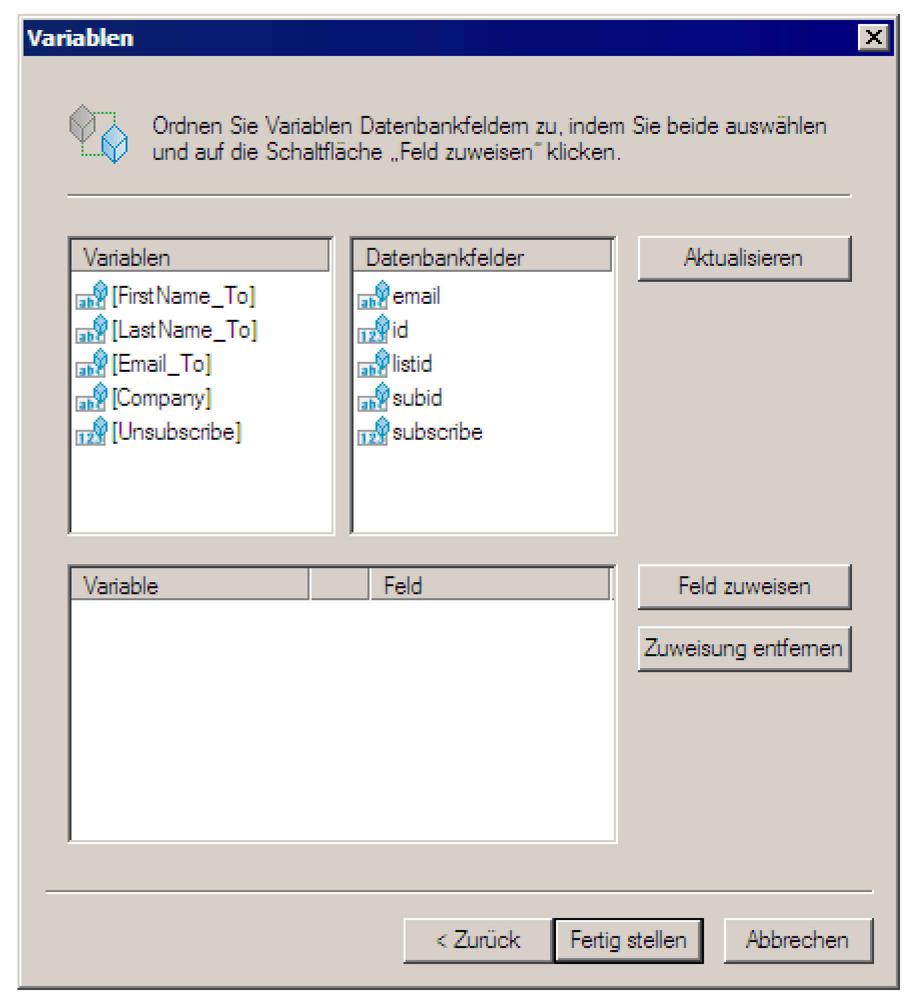


Bild 70 - Zuordnung benutzerdefinierter Felder

6. Wählen Sie eine Variable aus der Liste **Variablen** und klicken Sie auf die entsprechende Option **Datenbankfelder** sowie auf die Schaltfläche **Feld zuordnen** um die benötigten Felder den benutzerdefinierten Feldern in der Datenbank zuzuordnen. Klicken Sie auf **Fertigstellen** um Ihre Konfiguration zu übernehmen. Folgende Felder werden zugeordnet:

- **[Email_To]** - Zuordnung eines Text-String-Felds mit der E-Mail-Adresse eines Abonnenten.
- **[Unsubscribe]** - Zuordnung zu einem Feld mit einer Ganzzahl oder einem booleschen Wert, aus der/dem hervorgeht, ob der Benutzer in der Liste ein- oder ausgetragen ist.
- **[FirstName_To]** - Zuordnung eines Text-String-Felds mit dem

Vornamen eines Abonnenten.

- **[LastName_To]** - Zuordnung eines Text-String-Felds mit dem Nachnamen eines Abonnenten.
- **[Company]** - Zuordnung eines Text-String-Felds mit dem Namen der Firma eines Abonnenten.

4.5.2 Konfigurieren erweiterter Eigenschaften für Newsletter/Diskussionslisten

Sobald Sie eine neue Liste erstellt haben, können Sie weitere Optionen konfigurieren, beispielsweise Elemente und Verhalten der Liste benutzerspezifisch anpassen. Die verfügbaren Optionen sind:

- Erstellen einer benutzerdefinierten Fußzeile - Eine benutzerspezifische Fußzeile im HTML- oder Textformat konfigurieren. Dabei wird jeder E-Mail eine Fußzeile hinzugefügt.
- Einstellen von Berechtigungen für die Liste - Geben Sie an, wer E-Mails an die Liste senden darf. Wenn die Liste nicht gesichert ist, kann jeder eine E-Mail an die komplette Liste senden, indem er eine E-Mail an die Listenadresse schickt.

  HINWEIS: Berechtigungen für Diskussionslisten lassen sich nicht konfigurieren.
- Sichern von Newslettern mit einem Kennwort - Newsletter/Diskussion mit Kennwort sichern - Legen Sie ein Kennwort fest, das den Zugriff auf den Newsletter/die Diskussionsliste sichert, falls jemand den Kontenzugriff eines zulässigen Benutzers oder dessen E-Mail Client verwendet.
- Hinzufügen von Abonnenten zur Liste - Ergänzen Sie Benutzer für Newsletter und Diskussionslisten, ohne dass diese etwas tun müssen.

Erstellen einer benutzerdefinierten Fußzeile für die Liste

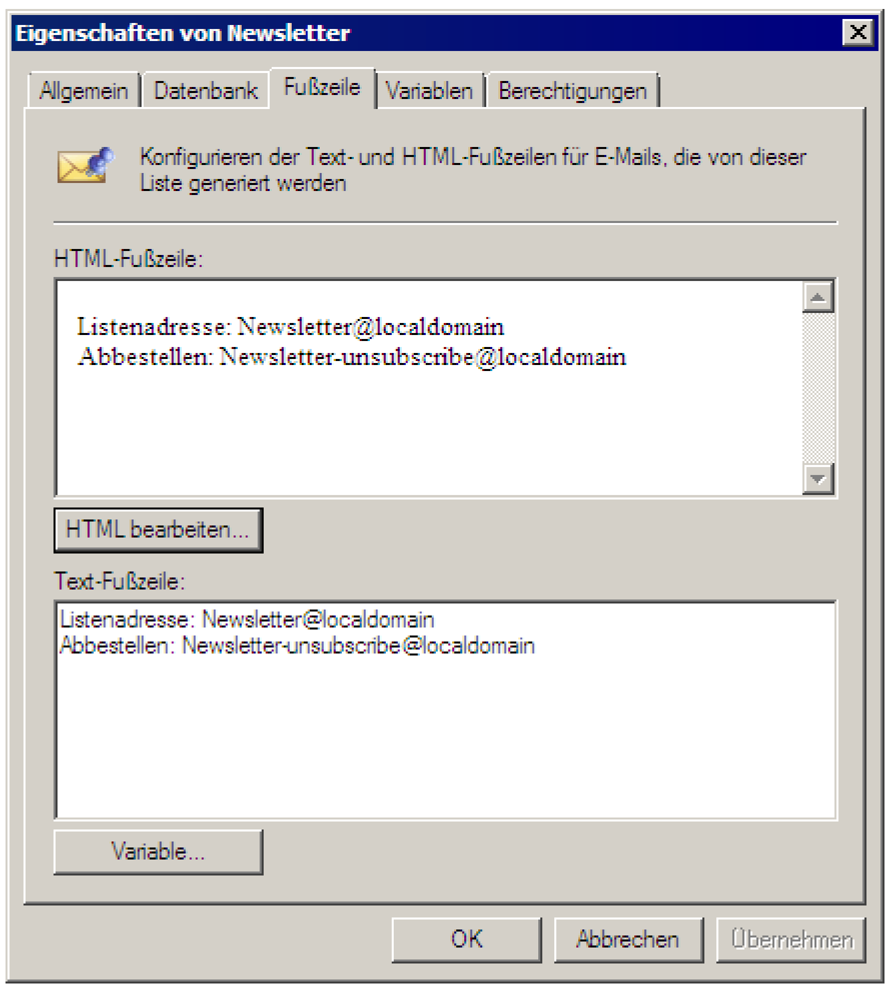


Bild 71 - Newsletter-Fußzeile - Eigenschaften

1. Klicken Sie mit der rechten Maustaste auf die Regel um eine Fußzeile einzufügen und dann auf **Eigenschaften**.

2. Klicken Sie auf der Registerkarte **Fußzeile** auf **HTML bearbeiten** um eine HTML-Fußzeile zu bearbeiten.

HINWEIS: Über die Fußzeile können Sie Benutzern die Möglichkeit einräumen, sich aus der Liste auszutragen und dort einzutragen.

Einstellen von Berechtigungen für die Liste

HINWEIS: Berechtigungen für Diskussionslisten lassen sich nicht konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

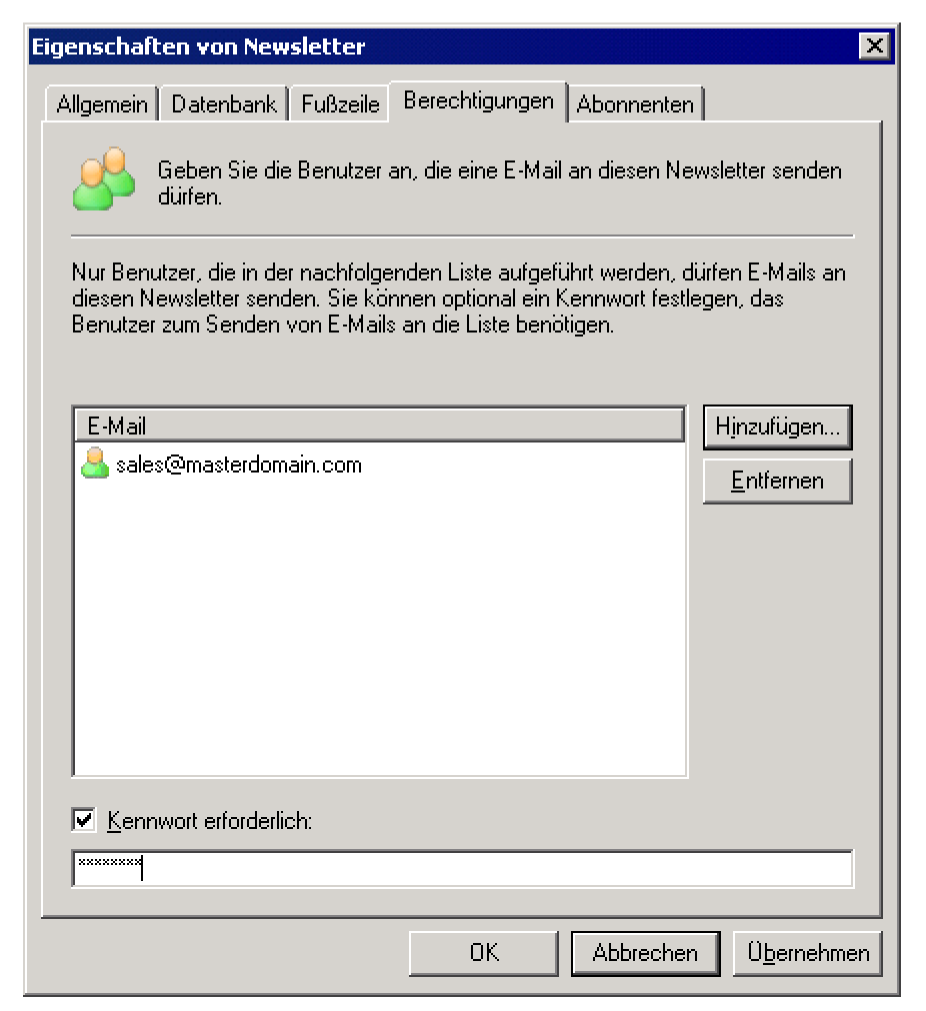


Bild 72 - Einstellen von Berechtigungen für die Liste

2. Klicken Sie auf der Registerkarte **Berechtigungen** auf die Schaltfläche **Hinzufügen** und geben Sie die Benutzer an, die berechtigt sind, eine E-Mail an die Liste zu senden. E-Mail-Adressen werden in der **E-Mail**-Liste hinzugefügt.

3. Aktivieren Sie Kennwörter, indem Sie in das Kontrollkästchen **Kennwort erforderlich** klicken und ein Kennwort angeben. Weitere Informationen, wie Sie diese Funktion nutzen, finden Sie im nächsten Abschnitt: Sichern von Newslettern mit einem Kennwort.

Sichern von Newslettern mit einem Kennwort

HINWEIS: Diskussionslisten können nicht mit Kennwörtern geschützt werden.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

2. Klicken Sie auf der Registerkarte **Berechtigungen** in das Kontrollkästchen **Kennwort erforderlich:** und geben Sie ein Kennwort an.

WICHTIGER HINWEIS: Die Benutzer müssen sich authentifizieren, indem sie das Kennwort in der E-Mail-Betreffzeile eingeben, wenn sie E-Mails an den Newsletter senden. Dieses Kennwort muss im Betreff-Feld wie folgt

angegeben werden:

[KENNWORT:*<Kennwort:>***]** *<Betreff der E-Mail!>*

- **Beispiel:** [KENNWORT:letmepost]Sonderangebot.

Ist das Kennwort richtig, entfernt der Listenserver die Kennwortdaten aus der Betreffzeile und leitet die E-Mail an den Newsletter weiter.

Hinzufügen von Abonnenten zur Liste

HINWEIS: Die Benutzer müssen sich bei der Liste anmelden, indem sie eine E-Mail an die Anmeldeadresse für den Newsletter/die Diskussionsliste senden. Werden Benutzer ohne ihre ausdrückliche Zustimmung in Listen hinzugefügt, müssen Sie mit Beschwerden wegen Spam rechnen.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

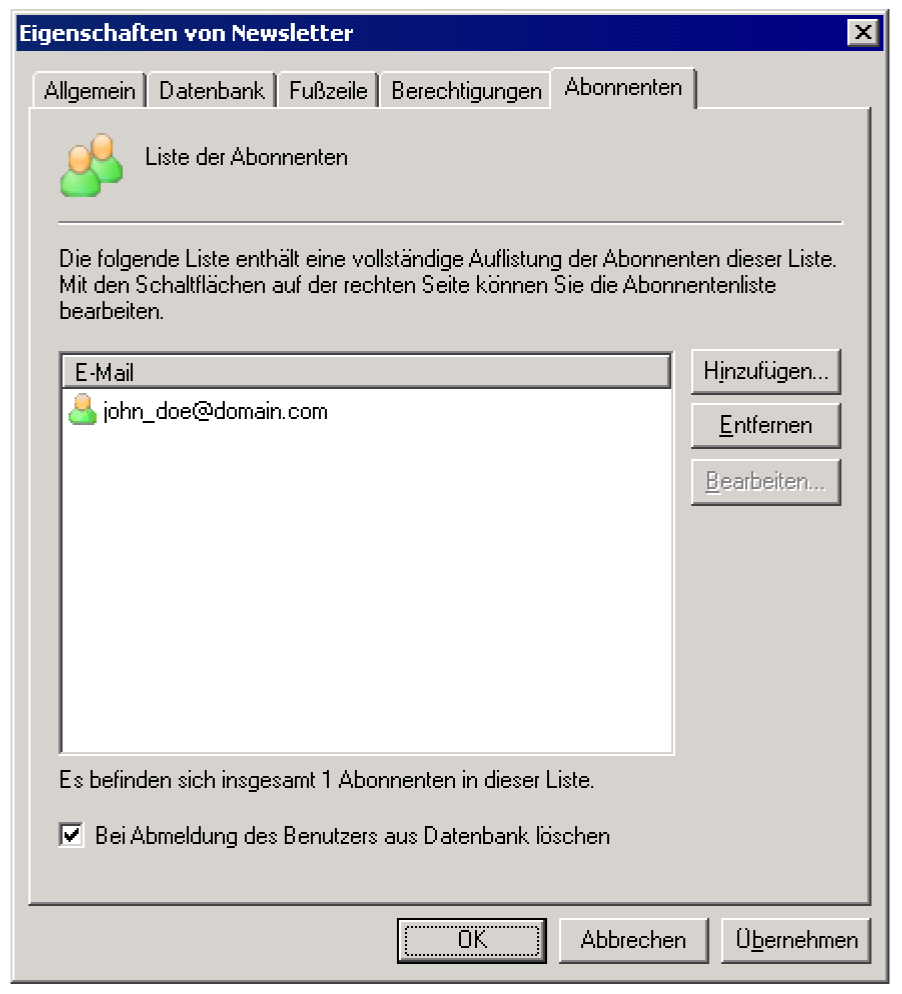


Bild 73 - Eingabe von Teilnehmern für den Newsletter

2. Klicken Sie auf der Registerkarte **Abonnenten** auf die Schaltfläche **Hinzufügen**.

3. Füllen Sie die Felder **E-Mail-Adresse**, **Vorname** und **Nachname** sowie **Firmendaten** aus und klicken Sie auf die Schaltfläche **OK**. Die neue Abonnenten-E-Mail-Adresse wird in der **E-Mail**-Liste hinzugefügt.

HINWEIS 1: Die Felder Vorname, Nachname und Firma sind optional.

HINWEIS 2: Wählen Sie den Benutzer aus und klicken Sie auf die Schaltfläche **Entfernen** um Abonnenten aus der Liste zu entfernen.

HINWEIS 3: Wenn Sie Benutzer aus der Abonnentenlistentabelle entfernen wollen, wenn diese sich von der Liste abmelden (und diese nicht nur als ausgetragen markieren) wollen, klicken Sie in das Kontrollkästchen **Bei Abmeldung des Benutzers aus Datenbank löschen.**

4.5.3 Einsatz von Newslettern/Diskussionslisten

Nach Anlage eines Newsletters/einer Diskussionsliste müssen die Benutzer sich anmelden, damit sie diese erhalten. Folgende Schritte können Benutzer für Newsletter/Diskussionslisten ausführen:

- Einen Newsletter lesen
- Sich bei einer Liste anmelden
- Die Anmeldung abschließen
- Einen Newsletter erstellen
- Sich aus der Liste austragen

Einsatz von Newslettern

- **Anmeldung bei der Liste** - Bitten Sie die Benutzer, eine E-Mail an <newslettername>-subscribe@yourdomain.com zu senden.
- **Abschluss der Eintragung** - Die Benutzer senden zunächst eine Bitte mit Eintragung in der Liste an <newslettername>-subscribe@yourdomain.com. Sobald diese Bitte empfangen wird, sendet der Listen-Server eine Bestätigungs-E-Mail zurück. Die Benutzer müssen ihre Eintragung über die Antwort-E-Mail bestätigen, damit sie als Abonnent ergänzt werden.

  HINWEIS: Die Bestätigungs-E-Mail ist obligatorisch und kann nicht abgeschaltet werden.
- **Versenden eines Newsletters/Diskussionslistenbeitrags -** Mitglieder, die die Berechtigung haben, E-Mails an die Liste zu senden, müssen die E-Mail an die E-Mail-Adresse des Newsletters senden: <newslettername>@yourdomain.com
- **Austragung aus der Liste** - Um sich aus der Liste auszutragen, müssen die Benutzer eine E-Mail an folgende E-Mail-Adresse senden: <newslettername>-unsubscribe@yourdomain.com

Tipp: Damit sich Benutzer einfach bei Newslettern anmelden können, sollten Sie ein Webformular mit Feldern für Name und E-Mail-Adresse und direkter Ausgabe an folgende Adresse ergänzen: <newslettername>-subscribe@yourdomain.com

4.5.4 Importieren von Abonnenten in die Liste/Datenbankstruktur

Wenn Sie einen neuen Newsletter oder eine neue Diskussionsliste erstellen, wird bei der Konfiguration eine Tabelle 'Listenname_Abonnenten' mit den unten angezeigten Feldern erstellt.

Um Daten in die Liste zu importieren, müssen Sie die Datenbank mit

den richtigen Daten in den richtigen Feldern füllen.

Feldname	Typ	Standard Wert	Kennzeichnungen	Beschreibung
Ls_id	Varchar(100)		PK	Abonnent-ID
Ls_first	Varchar(250)			Vorname
Ls_last	Varchar(250)			Nachname
Ls_email	Varchar(250)			E-Mail
Ls_unsubscribed	Int	0	NOT NULL	Austragungskennzeichnung
ls_company	Varchar(250)			Name der Firma

5 Verschiedenes

In diesem Abschnitt werden alle anderen Funktionen beschrieben, die nicht zur Erstkonfiguration, zur Routineverwaltung und zur kundenspezifischen Anpassung von GFI MailEssentials gehören.

5.1 Konfiguration von POP3 und Download-Einwahlverbindung

Das Post Office Protocol (POP3 nach RFC 1225) ist ein Client Server-Protokoll zur Speicherung von E-Mails, damit Clients eine Verbindung mit dem POP3-Server jederzeit aufbauen und die E-Mails lesen können. Ein Mail Client stellt die TCP/IP-Verbindung mit dem Server her, sodass die Benutzer nach Austausch verschiedener Befehle die E-Mail lesen können. Alle ISPs unterstützen POP3.

Wir empfehlen für GFI MailEssentials, POP3 möglichst nicht zu verwenden, sondern SMTP, da POP3 für E-Mail Clients konzipiert ist und nicht für Mail-Server. Trotzdem kann es Situationen geben, in denen eine statische IP-Adresse für SMPT nicht verfügbar ist, daher kann GFI MailEssentials E-Mails über POP3 abholen.

5.1.1 Konfiguration des POP3-Downloaders

1. Klicken Sie auf den Knoten **POP2Exchange** und doppelklicken Sie auf den Eintrag **Allgemein**.

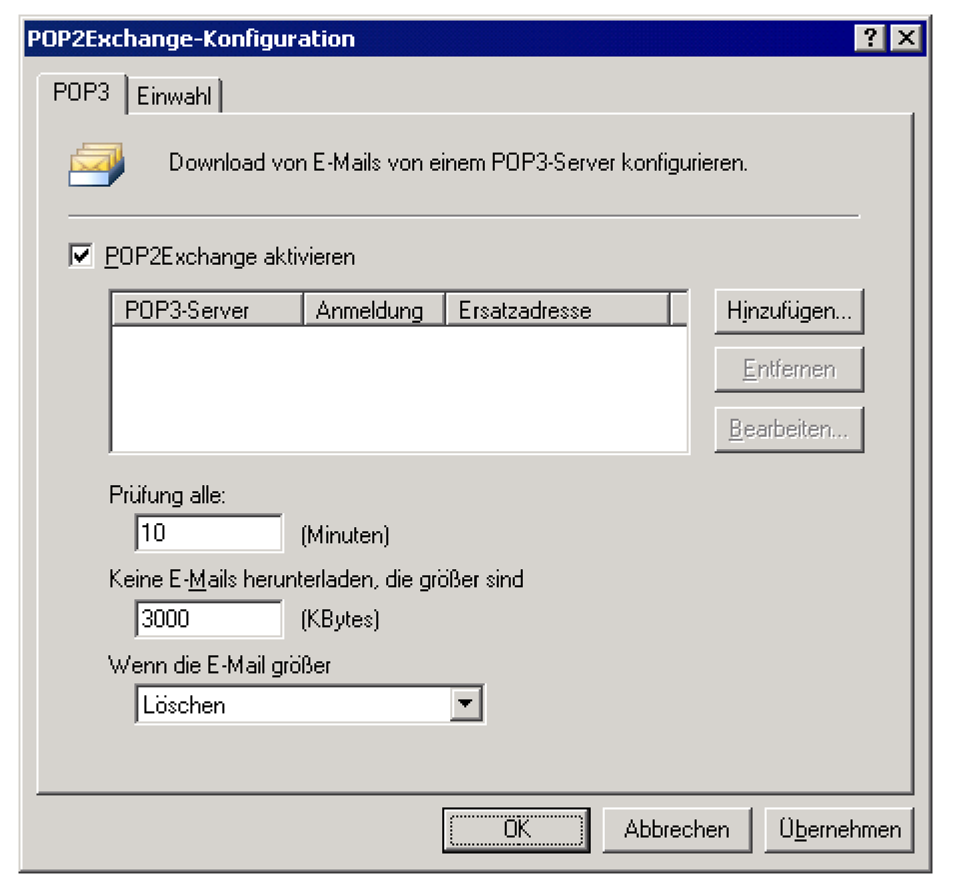


Bild 74 - POP3-Downloader von GFI MailEssentials

2. Klicken Sie auf der Registerkarte **POP3** in das Kontrollkästchen **POP2Exchange** aktivieren um den POP3-Downloader zu aktivieren.

3. Klicken Sie auf **Hinzufügen** um eine POP3-Mail-Box hinzuzufügen, in die E-Mails heruntergeladen werden.



Bild 75 - Hinzufügen eines POP3- Postfachs

4. Geben Sie die POP3-Serverdetails, den Benutzernamen und das Kennwort für das Postfach ein. Wählen Sie zwischen folgenden Optionen:

- **Mail an die in dem Feld 'To' gespeicherte E-Mail-Adresse senden -** GFI MailEssentials analysiert den E-Mail-Header und leitet die E-Mail entsprechend um. Wenn die E-Mail-Analyse fehlschlägt, wird die E-Mail an eine in dem Feld Ersatzadresse angegebene E-Mail-Adresse gesendet.
- **Mail an Ersatzadresse senden:** Alle E-Mails aus diesem Postfach werden an eine E-Mail-Adresse weitergeleitet. Geben Sie die vollständige SMTP-Adresse in dem Feld 'E-Mail-Adresse' ein.
  - **Beispiel:** john@company.com

5. Geben Sie die Ersatzadresse ein und klicken Sie auf **OK**.

HINWEIS 1: Wenn Sie die Zieladresse angeben (die Adresse, an die GFI MailEssentials die E-Mail weiterleitet), müssen Sie kontrollieren, ob Sie die betreffende SMTP-Adresse auf Ihrem Mailserver konfiguriert haben.

HINWEIS 2: Es können mehrere POP3 -Postfächer konfiguriert werden.

6. Konfigurieren Sie in dem Konfigurationsdialog POP2Exchange die anderen verfügbaren Optionen:

- **In folgendem Intervall prüfen (Minuten):** Definieren Sie das Intervall zum Herunterladen.
- **Keine E-Mail herunterladen, die größer ist als (Kilobyte):** Geben Sie die maximale Datengröße für das Herunterladen an. Wenn die E-Mail größer ist, wird sie nicht heruntergeladen.

- **Bei größerer E-Mail wie folgt verfahren:** Löschen Sie E-Mails, die größer sind als maximal zulässig, oder senden Sie eine Nachricht an den Postmaster.

5.1.2 Einwahl-Verbindungsoptionen konfigurieren

1. Klicken Sie auf den Knoten **POP2 Exchange** und doppelklicken Sie auf den Eintrag **Allgemein**.

2. Klicken Sie auf der Registerkarte **Einwahl** in das Kontrollkästchen **E-Mails per automatischer Einwahl oder bei Bedarf empfangen** um die Einwahlverbindung zu aktivieren.

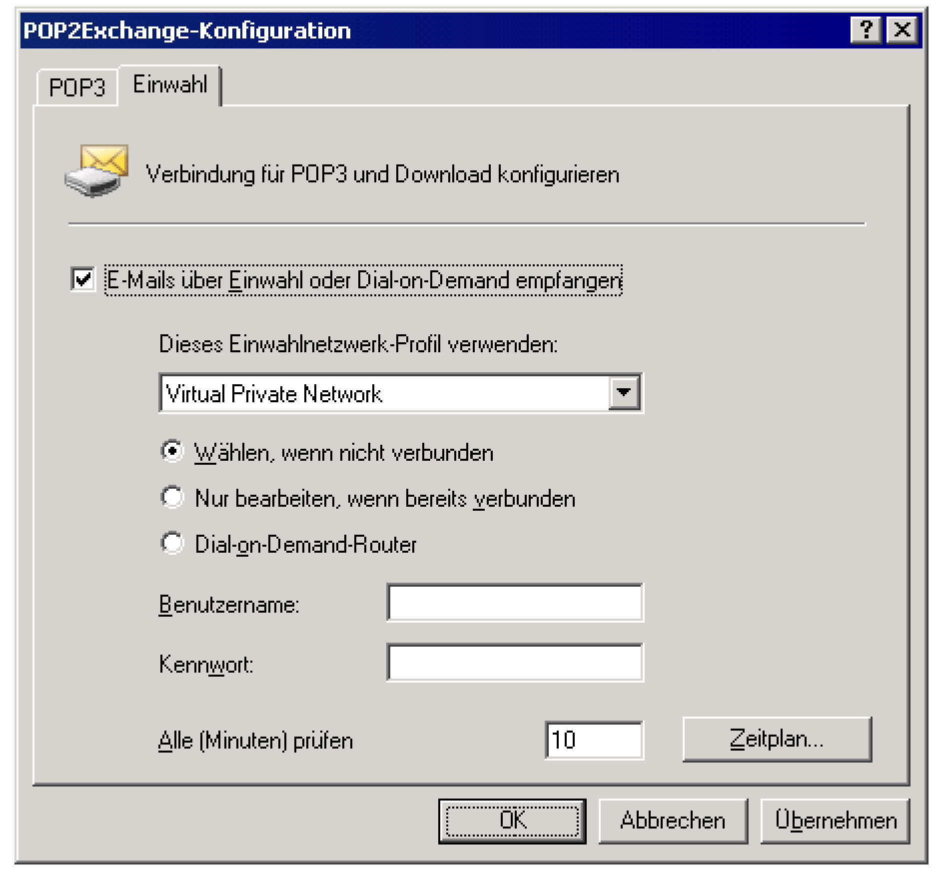


Bild 76 - Einwahloptionen

3. Wählen Sie ein Einwahlnetzwerkprofil aus und konfigurieren Sie einen Benutzernamen und ein Kennwort. Folgende Optionen sind verfügbar:

- **Dieses Einwahlnetzwerkprofil verwenden:** Wählen Sie, welches Einwahlnetzwerkprofil verwendet werden soll.
- **Einwahl, wenn keine Verbindung vorhanden:** GFI MailEssentials benutzt die Einwahlverbindung nur dann, wenn keine Verbindung existiert.
- **Benutzername:** Geben Sie den verwendeten Benutzernamen für die Anmeldung bei ISP ein.
- **Kennwort:** Geben Sie das Kennwort für die Anmeldung bei Ihrem ISP ein.
- **Nur verarbeiten, wenn Verbindung vorhanden:** GFI MailEssentials verarbeitet E-Mails nur dann, wenn bereits eine

Verbindung existiert.

- **Bei Bedarf über Router einwählen:** Falls eine Internetverbindung vorhanden ist, die automatisch hergestellt wird (beispielsweise nach Bedarf bei Einwahl über einen Router), wählen Sie diese Option aus. GFI MailEssentials holt die E-Mails in den definierten Zeitabständen ab, ohne selbst eine Einwahlverbindung aufzubauen.
- **Alle (Minuten) bearbeiten):** Geben Sie ein, wie oft GFI MailEssentials eine Einwahlverbindung herstellen oder prüfen soll, ob bereits eine Verbindung existiert (je nachdem, ob Sie GFI MailEssentials für eine Einwahlverbindung konfigurieren oder E-Mails nur verarbeitet werden sollen, wenn bereits eine Verbindung existiert).

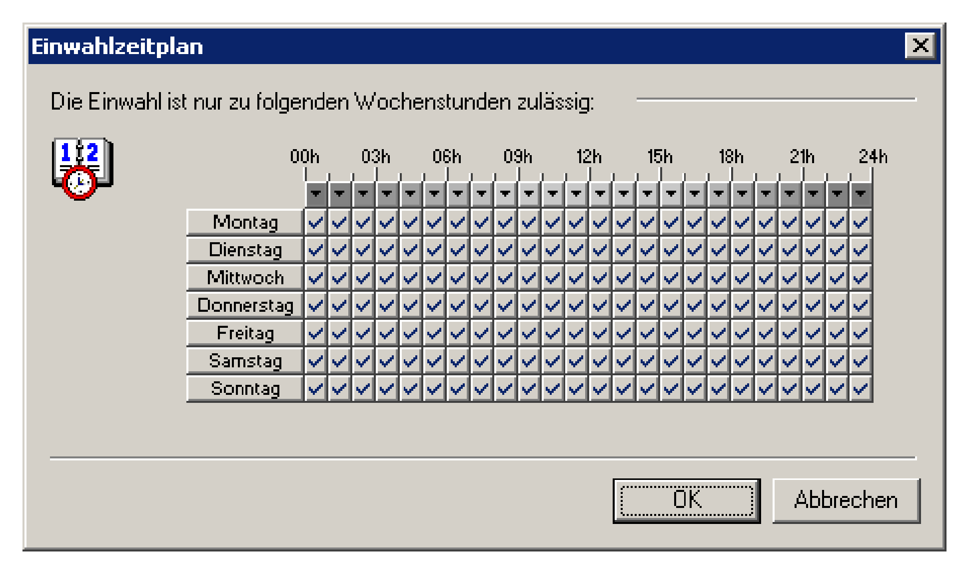


Bild 77 - Konfiguration der E-Mail-Abholung durch GFI MailEssentials

4. Klicken Sie auf **Zeitplan** und geben Sie an, zu welcher Uhrzeit GFI MailEssentials eine Einwahlverbindung herstellen und E-Mails abholen soll. Ein Häkchen gibt an, dass GFI MailEssentials eine Einwahlverbindung herstellt. Ein Kreuz gibt an, dass GFI MailEssentials in dieser Stunde keine Einwahlverbindung herstellt.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

5.2 E-Mail-Überwachung

E-Mail-Überwachung erlaubt den Versand von Kopien der von/an bestimmte lokale E-Mail-Adressen gesendeten E-Mails an eine andere E-Mail-Adresse. Auf diese Weise können Sie zentrale Speicher der E-Mail-Kommunikation für bestimmte Personen oder Abteilungen anlegen.

Sie können diese Funktion auch als Ersatz für eine E-Mail-Archivierung benutzen, da die E-Mails automatisch an Microsoft Exchange Server oder Microsoft Outlook gesendet werden.

5.2.1 Aktivieren/Deaktivieren der E-Mail-Überwachung

1. Klicken Sie mit der rechten Maustaste auf **E-Mail-Verwaltung ► E-Mail-Überwachung** und dann auf **Eigenschaften**.

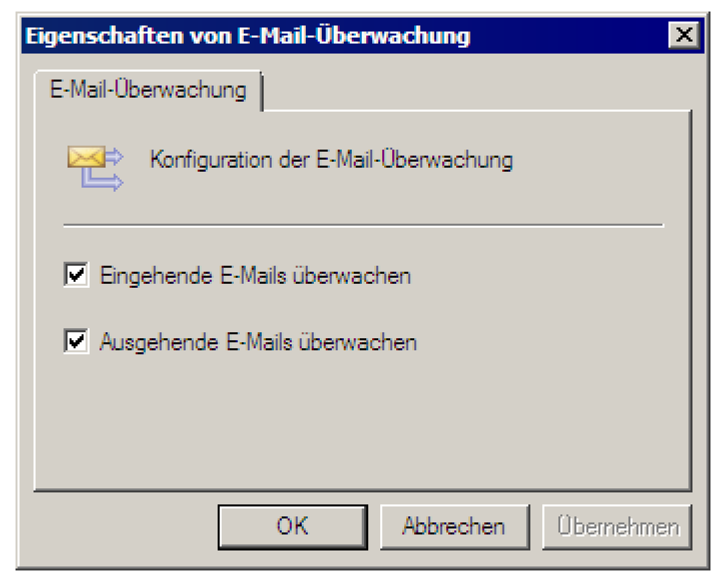


Bild 78 - E-Mail-Überwachung aktivieren oder deaktivieren

2. Aktivieren/deaktivieren Sie alle Überwachungsregeln für eingehende und ausgehende E-Mails, indem Sie die Kontrollkästchen **Eingehende Überwachung aktivieren** und **Ausgehende Überwachung aktivieren** deaktivieren oder aktivieren.

3. Klicken Sie auf **OK** um die Änderungen zu speichern.

HINWEIS: Aktivieren/deaktivieren Sie die Regeln zur Überwachung einzelner E-Mails, indem Sie mit der rechten Maustaste auf die Regeln zur E-Mail-Überwachung klicken, und dann die Option **Aktivieren/Deaktivieren** auswählen.

5.2.2 E-Mail-Überwachung konfigurieren

1. Klicken Sie mit der rechten Maustaste auf **E-Mail-Verwaltung ► E-Mail-Überwachung** und dann auf **Neu ► Überwachungsregel für eingehende Post oder** E-Mail-Überwachungsregel für ausgehende Post um eingehende oder ausgehende Post entsprechend zu überwachen.

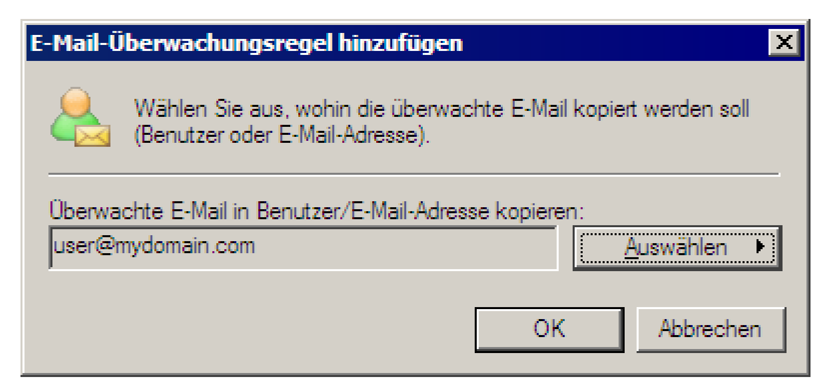


Bild 79 - E-Mail-Überwachungsregel hinzufügen

2. Geben Sie die Ziel-E-Mail-Adresse/das Zielpostfach an, in das E-Mails kopiert werden sollen. Klicken Sie auf **OK** um fortzufahren.

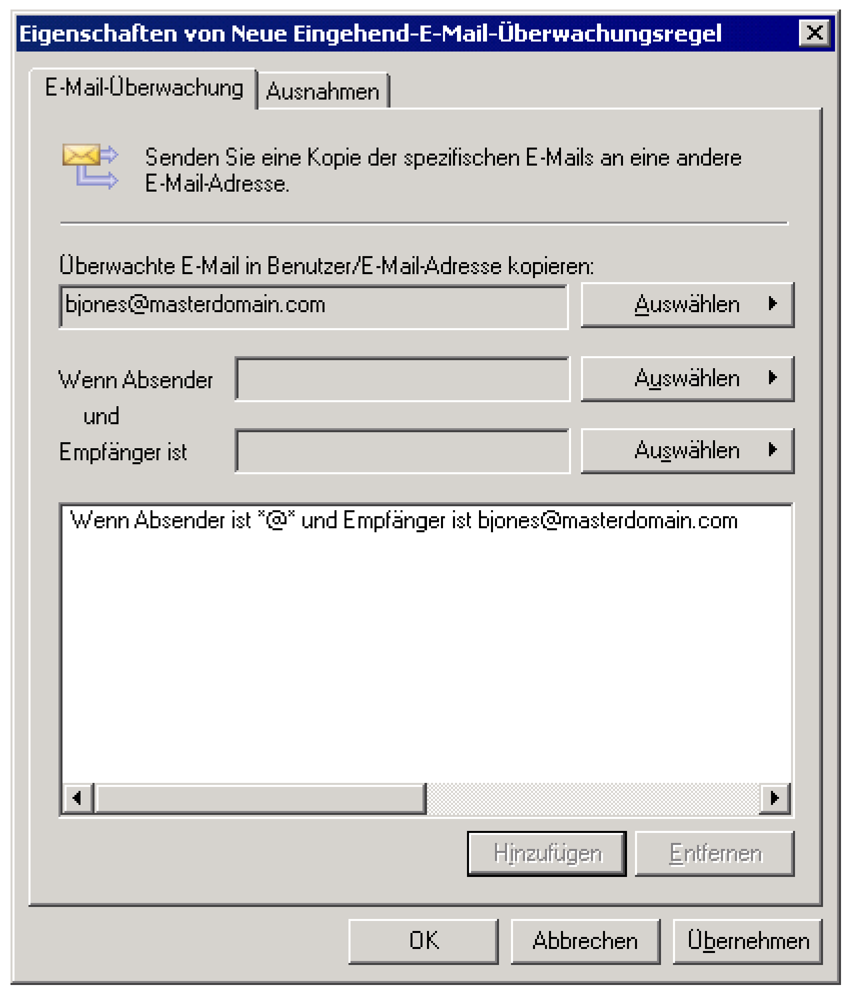


Bild 80 - Konfiguration der E-Mail-Überwachung

3. Klicken Sie auf Absender und Empfänger**. Wählen Sie mit den** Schaltflächen aus, welche E-Mails mit dieser Regel überwacht werden sollen. Klicken Sie auf **Hinzufügen** um Filter in der Liste hinzuzufügen. Wiederholen Sie die Schritte um mehrere Filter zu definieren. Die folgenden Bedingungen können überwacht werden:

HINWEIS: Wenn Sie alle E-Mails überwachen wollen, geben Sie *@* ein.

- **Alle von einem bestimmten Benutzer versendeten E-Mails** - Erstellen Sie eine Regel für ausgehende E-Mails, geben Sie die E-Mail des Absenders an oder wählen Sie den Benutzer (wenn Sie Active Directory verwenden) im Absenderfeld aus und geben Sie *@* als Domäne des Empfängers an.
- **Alle E-Mails, die an einen bestimmten Benutzer versendet werden**- Erstellen Sie eine Regel für eingehende E-Mails, definieren Sie in dem Empfängerfeld die E-Mails des Empfängers oder wählen Sie den Benutzer (wenn Sie Active Directory verwenden) aus und geben Sie *@* als Domäne des Absenders an.
- **Von einem bestimmten Benutzer gesendete E-Mail an einen externen Empfänger -** Erstellen Sie eine Regel für ausgehende E-Mails und geben Sie den Absender an oder wählen Sie den Benutzer bei Verwendung von Active Directory im Feld "Absender" aus. Geben Sie die E-Mail des externen Empfängers im Empfängerfeld ein.
- **Von einem externen Absender an einen bestimmten Benutzer gesendete E-Mail -** Erstellen Sie eine Regel für eingehende E-Mail und geben Sie in dem Feld "Absender" die E-Mail-Adresse des externen Absenders an. Geben Sie im Feld "Empfänger" den Benutzernamen oder die E-Mail-Adresse des Benutzers ein.
- **Von einem bestimmten Benutzer an eine Firma oder Domäne gesendete E-Mail -** Erstellen Sie eine Regel für ausgehende E-Mail und geben Sie den Absender bzw. den Benutzer (bei Verwendung von Active Directory) in dem Feld "Absender" ein. Geben Sie die Domäne der Firma in dem Feld "Empfänger" ein, indem Sie die **Domäne** über die Schaltfläche **Empfänger** auswählen.
- **Von einer Firma oder Domäne an bestimmte Benutzer gesendete E-Mail -** Erstellen Sie eine Regel für eingehende E-Mail und geben Sie die Domäne der Firma im Feld "Absender" ein. Wählen Sie die **Domäne** durch Klicken auf die Schaltfläche **Absender** aus und geben Sie den Benutzernamen bzw. die E-Mail-Adresse des Benutzers im Feld "Empfänger" ein.

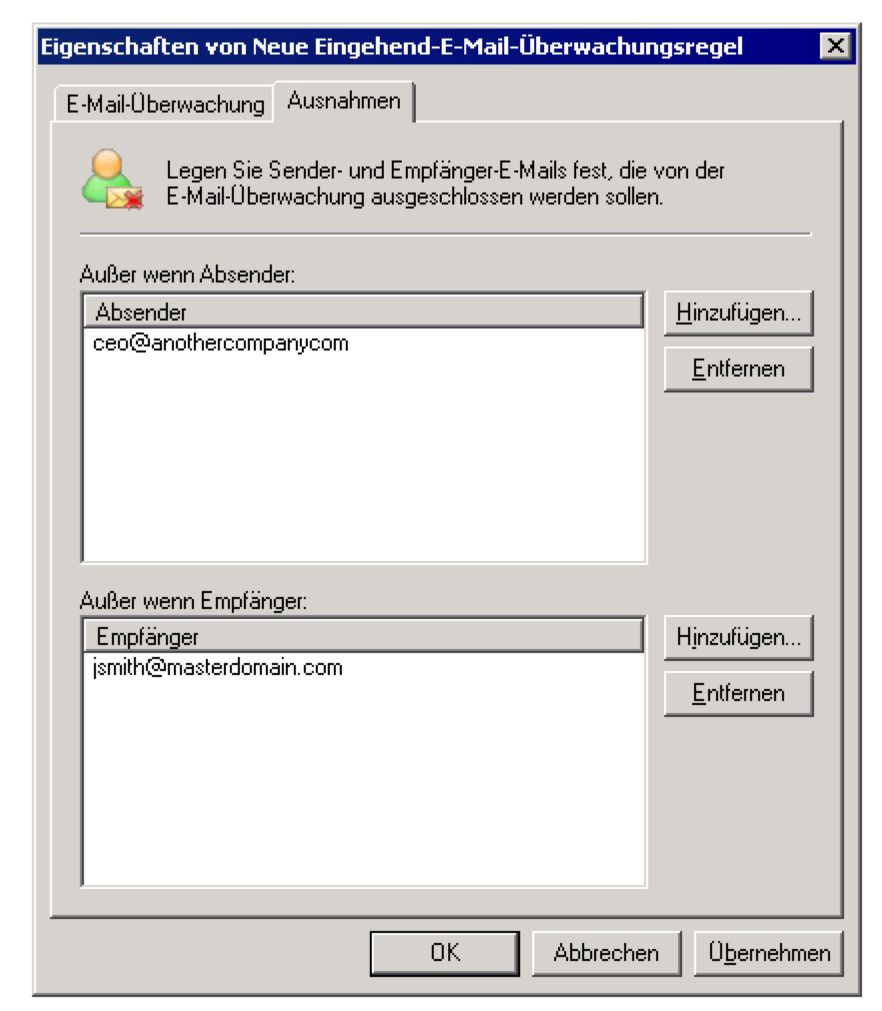


Bild 81 - Erstellen einer Ausnahme

4. Klicken Sie auf die Registerkarte Ausnahmen um Absender oder Empfänger hinzuzufügen, die bei der neuen Regel nicht berücksichtigt werden sollen. Die verfügbaren Optionen sind:

- **Außer wenn Absender gleich** - Schließt den angegebenen Absender aus der Liste aus.
- **Außer wenn Empfänger gleich** - Schließt den angegebenen Empfänger aus der Liste aus.

HINWEIS 1: Bei der Definition von Ausnahmen für Überwachungsregeln eingehender E-Mails enthält die **Absenderliste** nicht-lokale E-Mail-Adressen und die **Empfängerliste** nur lokale E-Mail-Adressen. Bei der Definition von Ausnahmen für eine Überwachungsregel ausgehender E-Mails enthält die **Absenderliste** lokale E-Mail-Adressen und die **Empfängerliste** nur nicht-lokale E-Mail-Adressen.

HINWEIS 2: Es werden beide Ausnahmelisten berücksichtigt und die in der Absender-Ausnahmeliste enthaltenen Absender sowie alle in der Empfänger-Ausnahmeliste enthaltenen Empfänger werden nicht überwacht.

5. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

HINWEIS: Eine neue E-Mail-Überwachungsregel können Sie umbenennen, indem Sie auf die E-Mail-Überwachungsregel klicken und dann die Taste F2 drücken.

5.3 Synchronisieren der Konfigurationsdaten

Wenn GFI MailEssentials auf mehr als einem Server installiert ist, müssen Sie die Anti-Spam- und KonfigurationsdatenKonfigurationsdaten zwischen den Servern synchronisieren, damit eine als Spam auf einem Server identifizierte E-Mail auch auf einem anderen Server als Spam-Mail identifiziert wird, wenn sie dorthin gelangt.

GFI MailEssentials automatisiert diesen Vorgang durch zwei Funktionen, mit denen sich mehrere Installationen von GFI MailEssentials synchronisieren lassen:

- Konfiguration des Anti-Spam Synchronization Agent: Dieser Dienst synchronisiert die Anti-Spam-Einstellungen verschiedener Installationen von GFI MailEssentials mit dem Microsoft BITS-Dienst.

  Der Anti-Spam Synchronization Agent arbeitet wie folgt:

  1. Ein Server, der als Host für GFI MailEssentials dient, ist als Master-Server konfiguriert.

  2. Die anderen Server, auf denen GFI MailEssentials installiert ist, sind als Slave-Server konfiguriert.

  3. Die Slave-Server laden eine Archivdatei mit den Anti-Spam-Einstellungen in einen virtuellen IIS-Ordner auf dem Master-Server über den BITS-Dienst hoch.

  4. Wenn der Master-Server alle Anti-Spam-Daten der Slave-Server erfasst hat, werden die Daten aus den einzelnen Archiven extrahiert und in einer neuen aktuellen Archivdatei für die Anti-Spam-Einstellungen zusammengeführt.

  5. Die Slave-Server laden diese aktualisierte Archivdatei mit den Anti-Spam-Einstellungen herunter, extrahieren sie und aktualisieren die lokale Installation von GFI MailEssentials mit den neuen Einstellungen.

  HINWEIS 1: Bei allen Servern, die zur Synchronisation der Anti-Spam-Einstellungen zusammenarbeiten, muss mindestens GFI MailEssentials 14.1 installiert sein.

  HINWEIS 2: Die durch den Anti-Spam Synchronization Agenten hochgeladenen und heruntergeladenen Dateien sind komprimiert um den Traffic im Netzwerk zu begrenzen.

  Ausführliche Hinweise zur Konfiguration des Anti-Spam Synchronization Agent finden Sie auf Seite 112 in diesem Handbuch.

- Konfiguration des GFI MailEssentials Export/Import-Tools: Mit dieser Anwendung können alle Konfigurationseinstellungen von GFI MailEssentials exportiert und importiert werden; die Konfiguration einer neuen Installation von GFI MailEssentials kann mit genau denselben Einstellungen wie bei einer funktionsfähigen Installation von GFI MailEssentials erfolgen.

5.3.1 Konfiguration des Anti-Spam Synchronization Agent

Für den Anti-Spam Synchronization Agenten müssen Sie die folgenden Schritte in folgender Reihenfolge ausführen:

Schritt 1: Konfigurieren Sie den Master-Server.

Schritt 2: Installieren Sie die BITS-Server-Erweiterung auf dem Master-Server.

Schritt 3: Konfigurieren Sie den Slave-Server.

5.3.2 Konfiguration des Master-Servers

Wichtige Hinweise

1. Es kann immer nur ein Server als Master-Server konfiguriert werden.

2. Ein Server muss folgende Systemspezifikationen erfüllen, wenn er als Master-Server konfiguriert werden soll:

- Microsoft Windows Server 2003 mit SP1 oder höher und IIS6.0 mit installierter BITS-Server-Erweiterung. (Weitere Informationen zur Installation der BITS-Server-Erweiterung finden Sie weiter unten.)
- Microsoft Windows 2000 mit SP3 oder höher und IIS5.0 mit installierter BITS-Server-Erweiterung. (Weitere Informationen zur Installation der BITS-Server-Erweiterung finden Sie weiter unten.)

HINWEIS: Ein Computer mit Microsoft Windows XP kann nicht als Master-Server konfiguriert werden, da die Microsoft BITS-Server-Erweiterung nicht unterstützt wird.

Konfiguration des Master-Servers

1. Installieren Sie die Microsoft BITS-Server-Erweiterung. Weitere Informationen finden Sie im Abschnitt Installieren der BITS-Server-Erweiterung auf dem Master-Server finden Sie auf Seite 115 in diesem Handbuch.

2. Laden Sie über die Gruppe **Administrator Tools** die Konsole **Internet Informationsdienste Manager (IIS)**, klicken Sie mit der rechten Maustaste auf die gewünschte Website und dann im Kontextmenü auf **Neu ► Virtuelles Verzeichnis.**

3. Führen Sie den **Assistenten zum Erstellen des virtuellen Verzeichnisses** aus, und erstellen Sie ein neues virtuelles Verzeichnis.

HINWEIS: Achten Sie darauf, dass nur die Kontrollkästchen **Lesen** und **Schreiben** aktiviert und alle anderen Kontrollkästchen deaktiviert sind.

4. Klicken Sie mit der rechten Maustaste auf das neue virtuelle Verzeichnis und dann auf **Eigenschaften**. Klicken Sie auf die Registerkarte **Verzeichnissicherheit** und dann auf **Bearbeiten** in der Gruppe **Authentifizierung und Zugriffskontrolle**.

5. Klicken Sie in das Kontrollkästchen **Basisauthentifizierung**, und geben Sie die **Standarddomäne** sowie den **Bereich** an, zu dem der Benutzername und das Kennwort für die Authentifizierung der Slave-Computer gehören.

HINWEIS: Kontrollieren Sie, dass alle anderen Kontrollkästchen deaktiviert sind.

6. Klicken Sie auf **OK**, und schließen Sie den Dialog **Authentifizierungsverfahren**.

7. Rufen Sie die Registerkarte **BITS Server-Erweiterung** auf, und klicken Sie in das Kontrollkästchen **Clients dürfen Daten in dieses virtuelle Verzeichnis übertragen**.

8. Klicken Sie auf **Start ► GFI MailEssentials ► GFI MailEssentials Anti-Spam Synchronization Agent**, und klicken Sie dann mit der rechten Maustaste auf den Knoten **Anti-Spam Synchronization Agent ► Konfiguration** sowie auf **Eigenschaften**.

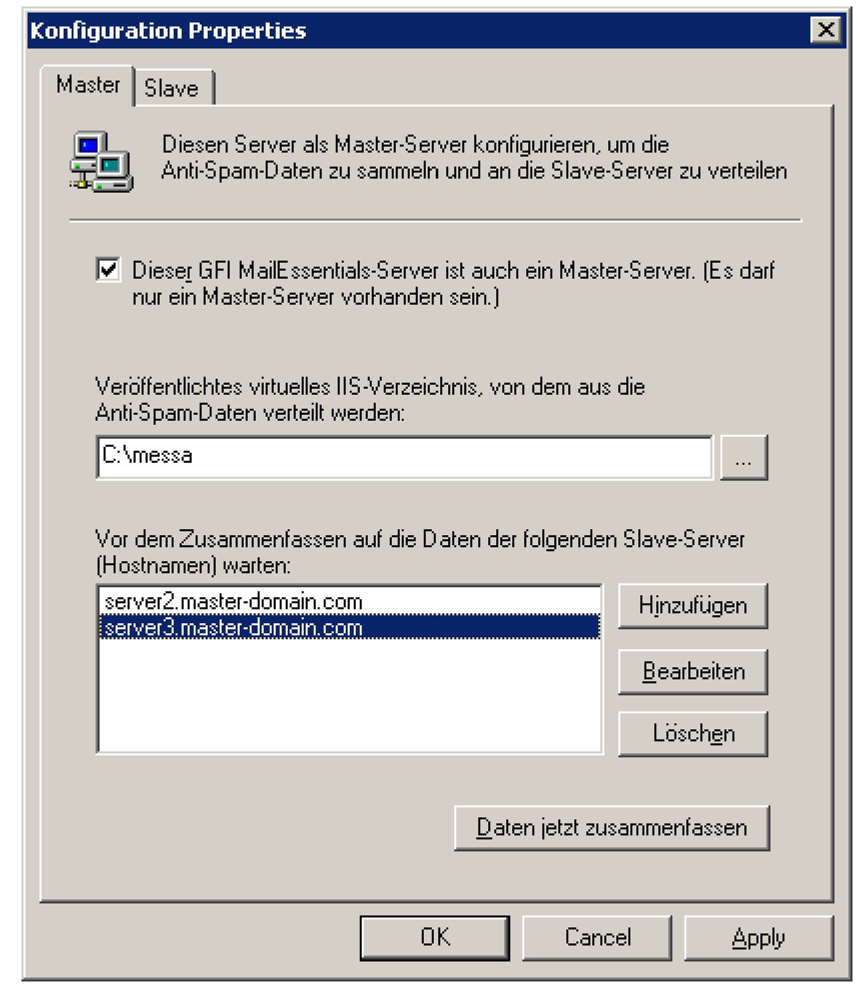


Bild 82 - Konfiguration eines Master-Servers

9. Klicken Sie auf der Registerkarte **Master** in das Kontrollkästchen **Dieser GFI-MailEssential-Server ist auch Master-Server**, und geben Sie den kompletten Pfad des Ordners ein, der den Inhalt des virtuellen Verzeichnisses aufnehmen soll.

10. Klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie den Host-Namen des Slave-Servers in dem Bearbeitungsfeld **Server** ein. Klicken Sie auf **OK** um den Server zur Liste hinzuzufügen. Wiederholen Sie diesen Schritt, und ergänzen Sie alle anderen konfigurierten Slave-Server.

HINWEIS 1: Achten Sie darauf, dass Sie alle Computer konfigurieren, die Sie in dieser Liste als Slave-Server hinzufügen, da sonst der Anti-Spam Synchronization Agent des Master-Servers niemals die Daten zusammenführen kann.

HINWEIS 2: Ein Master-Server kann gleichzeitig auch Slave-Server sein. In diesem Fall führt der Server seine eigenen Anti-Spam-

Einstellungen mit den hochgeladenen Einstellungen der anderen Slave-Server zusammen. Damit diese Option funktioniert, müssen Sie den Master-Server-Host-Namen ebenfalls zur Liste der Slave-Server hinzufügen. Weitere Informationen finden Sie im Abschnitt Konfigurieren Sie den Slave-Server finden Sie auf Seite 115 in diesem Handbuch.

11. Wählen Sie bei Bedarf einen Slave-Server aus der Liste, und klicken Sie auf die Schaltfläche **Bearbeiten** oder **Löschen** um diesen zu bearbeiten oder zu löschen.

12. Klicken Sie auf die Schaltfläche **OK** um die Einstellungen zu speichern.

5.3.3 Installation der BITS-Server-Erweiterung auf dem Master-Server

1. Laden BITS V1.5 Serverkomponente von Microsoft herunter, und starten Sie diese auf dem Master-Server von:

http://www.microsoft.com/downloads/details.aspx?FamilyID=17967848-be86-4cd6-891c-ec8241611ad4&displaylang=de

2. Folgen Sie den Anweisungen des **BITS-Server-Konfigurationsassistenten** um die Installation abzuschließen.

3. Laden Sie von der **Systemsteuerung** aus die Registerkarte **Programme hinzufügen oder entfernen**, und klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**.

4. Klicken Sie in dem Dialog **Windows-Komponenten-Assistent** auf **Anwendungsserver** in der Liste **Komponenten** und dann auf **Details**.

4. Klicken Sie im Dialog für den **Anwendungsserver** auf **Internet Information Services (IIS)** in der Liste **Subkomponenten des Anwendungsservers**, und klicken Sie dann auf **Details**.

5. Klicken Sie in das Kontrollkästchen **Intelligenter Hintergrund-Übertragungsdienst (BITS) Servererweiterung** unter **Subkomponenten der Internet Information Services (IIS)** Liste und klicken Sie dann auf **OK**.

6. Klicken Sie auf **OK** um den Dialog **Anwendungsserver** zu schließen.

7. Klicken Sie im Dialog **Windows-Komponenten-Assistent** auf **Weiter** um die Installation zu beginnen.

8. Klicken Sie danach auf **Fertigstellen** um den **Windows-Komponenten-Assistenten** zu schließen.

5.3.4 Konfiguration eines Slave-Servers

Wichtige Hinweise

Zur Konfiguration eines Servers als Slave-Server muss dieser folgende Systemspezifikationen erfüllen:

- Microsoft Windows 2003 - Wir empfehlen Ihnen, das BITS 2.0 Client-Update über folgenden Link von Microsoft herunterzuladen:

  http://www.microsoft.com/downloads/details.aspx?familyid=3FD31F05-D091-49B3-8A80-BF9B83261372&displaylang=de

- Microsoft Windows 2000 mit SP3 oder höher - Sie müssen den BITS 2.0 Client über folgenden Link von Microsoft herunterladen:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=3ee866a0-3a09-4fdf-8bdb-c906850ab9f2&DisplayLang=de
- Microsoft Windows 2.0 mit SP3 oder höher - Sie müssen den BITS 2.0 Client über folgenden Link von Microsoft herunterladen:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=b93356b1-ba43-480f-983d-eb19368f9047&DisplayLang=de

Slave-Server-Konfiguration

1. Klicken Sie auf **Start ► GFI MailEssentials ► GFI MailEssentials Anti-Spam Synchronization Agent**.

2. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam Synchronization Agent ► Konfiguration** und dann auf **Eigenschaften**.

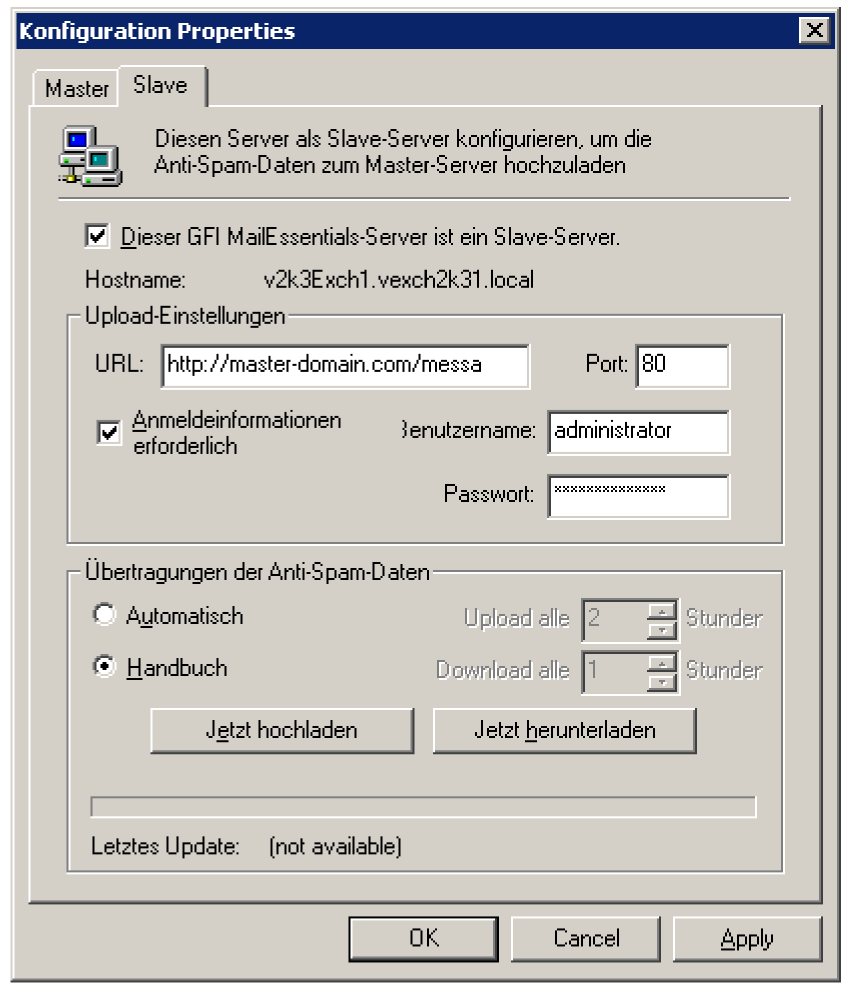


Bild 83 - Konfiguration eines Slave-Servers

3. Klicken Sie auf der Registerkarte **Slave** in das Kontrollkästchen **Dieser GFI MailAssential-Server ist ein Slave-Server**, und geben Sie die komplette URL zu dem virtuellen Verzeichnis auf dem Master-Server auf dem Feld **URL** an.

- **Beispiel:** 'http://master-Domäne.com/messas'

4. Geben Sie in dem Feld **Port** den Port an, den der Master-Server für

die HTTP-Kommunikation verwendet.

HINWEIS: Voreingestellt ist der Port 80, der Standard-Port für HTTP.

5. Klicken Sie in das Kontrollkästchen **Authentifizierungsdaten erforderlich**, und geben Sie Benutzernamen und Kennwort zur Authentifizierung bei dem Master-Server ein.

6. Wählen Sie:

- **Manuell -** Die Archivdatei mit den Anti-Spam-Einstellungen manuell herunterladen und hochladen. Klicken Sie auf die Schaltfläche **Jetzt hochladen**, wenn Sie die Anti-Spam-Einstellungen des Slave-Servers zum Master-Server hochladen wollen. Klicken Sie auf die Schaltfläche **Jetzt herunterladen**, wenn Sie die aktualisierte, zusammengeführte Datei mit den Anti-Spam-Einstellungen vom Master-Server herunterladen wollen.

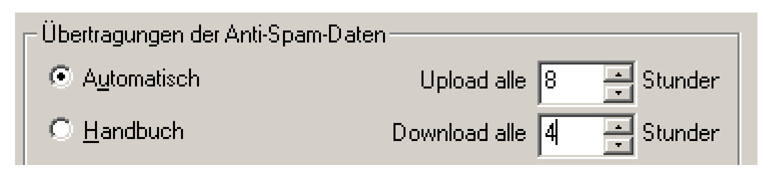


Bild 84 - Stundeneinstellung für das Hochladen/Herunterladen

- **Automatisch -** Konfiguriert die Anti-Spam-Synchronisation so, dass sie automatisch ausgeführt wird. Geben Sie in dem Feld **Hochladen alle** das Hochladeintervall in Stunden an; diese Einstellung legt fest, wie oft der Slave-Server seine Anti-Spam-Einstellungen zum Master-Server hochlädt. Geben Sie in dem Feld **Herunterladen alle** an, wie oft der Slave-Server auf dem Master-Server nach Aktualisierungen suchen und diese herunterladen soll.

HINWEIS: Das Stundenintervall für das Hochladen und Herunterladen dürfen Sie nicht auf den gleichen Wert einstellen. Für das Stundenintervall können Sie einen beliebigen Wert zwischen 1 und 240 Stunden wählen. Wir empfehlen Ihnen, das Intervall zum Herunterladen auf einen kleineren Wert einzustellen als das Intervall für das Hochladen und für alle konfigurierten Slave-Server die gleichen Intervalleinstellungen zu verwenden.

- **Beispiel:** Beispielsweise können Sie das Intervall zum Herunterladen auf drei Stunden und das Intervall zum Hochladen auf vier Stunden einstellen. Auf diese Weise werden Dateien öfter heruntergeladen als hochgeladen.

7. Klicken Sie auf die Schaltfläche **OK** um die Einstellungen zu speichern.

5.4 Konfiguration des GFI MailEssentials Export/Import-Tools

Für das Konfigurationsexport- und Import-Tool müssen Sie die folgenden Schritte in folgender Reihenfolge ausführen:

Schritt 1: Exportieren Sie die vorhandenen Konfigurationseinstellungen für GFI MailEssentials.

Schritt 2: Kopieren Sie per Hand die exportierten Einstellungen auf den Computer, auf dem Sie gerade GFI MailEssentials installiert

haben.

Schritt 3: Importieren Sie die Einstellungen in die neue Installation von GFI MailEssentials.

WICHTIGER HINWEIS: Beim Import von Einstellungen werden alle Installationseinstellungen von GFI MailEssentials auf der Zielinstallation überschrieben.

5.4.1 Exportieren der Konfigurationseinstellungen von GFI MailEssentials

GFI MailEssentials enthält zwei Verfahren zum Export der Konfigurationseinstellungen:

- Exportieren über die Benutzeroberfläche
- Exportieren von Einstellungen über die Befehlszeile

Exportieren über die Benutzeroberfläche

1. Doppelklicken Sie auf 'meconfigmrg.exe' im Hauptverzeichnis der Installation von GFI MailEssentials.

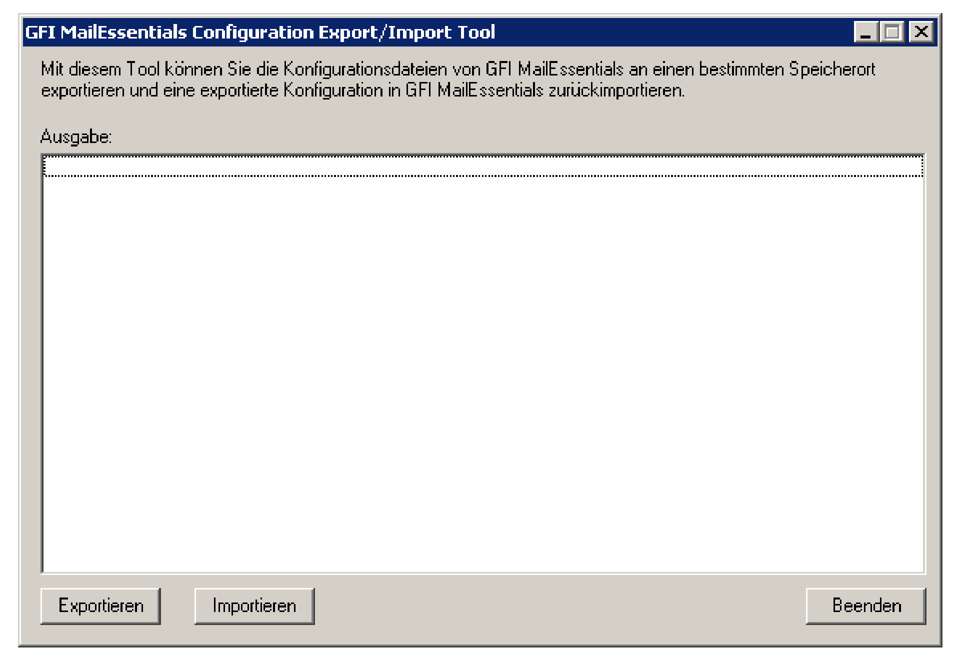


Bild 85 - Konfiguration des GFI MailEssentials Export/Import-Tools

2. Klicken Sie auf die Schaltfläche **Exportieren**. Wählen Sie in dem Dialog **Nach Ordner Suchen** einen Ordner aus, in den Sie die Konfigurationseinstellungen von GFI MailEssentials exportieren können, und klicken Sie auf **OK**.

3. Klicken Sie nach dem Abschluss auf die Schaltfläche **Beenden**.

Exportieren von Einstellungen über die Befehlszeile

1. Öffnen Sie eine Befehlszeile, und suchen Sie nach dem Installationshauptordner von GFI MailEssentials.

2. Geben Sie Folgendes ein:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

HINWEIS: Ersetzen Sie “C:\MailEssentials Settings” durch den gewünschten Zielpfad.

```
meconfigmgr.exe /export:"c:\MailEssentials Settings" /verbose /replace
[C:\Program Files\GFI\MailEssentials\config.mdb] wird kopiert -> [c:\MailEssentials Settings\config.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] wird kopiert -> [c:\MailEssentials Settings\autowhitelist.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\Data\weights.bsp] wird kopiert -> [c:\MailEssentials Settings\weights.bsp]
Fertig
[C:\Program Files\GFI\MailEssentials\userlist.mdb] wird kopiert -> [c:\MailEssentials Settings\userlist.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\pop2exchange.xml] wird kopiert -> [c:\MailEssentials Settings\pop2exchange.xml]
Fertig
[C:\Program Files\GFI\MailEssentials\spamord.xml] wird kopiert -> [c:\MailEssentials Settings\spamord.xml]
Fertig
[C:\Program Files\GFI\MailEssentials\Data\reports.mdb] wird kopiert -> [c:\MailEssentials Settings\reports.mdb]
Fertig
Fertig_
```

Bild 86 - Exportieren von Einstellungen über die Befehlszeile

- Der Parameter **/Verbose** weist das Tool an, beim Kopieren der Dateien den Arbeitsfortschritt anzuzeigen.
- Der Parameter **/Replace** weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.

5.4.2 Importieren der Konfigurationseinstellungen von GFI MailEssentials

GFI MailEssentials bietet zwei Verfahren zum Import der Konfigurationseinstellungen:

- Importieren über die Benutzeroberfläche
- Importieren über die Befehlszeile

Importieren über die Benutzeroberfläche

1. Doppelklicken Sie auf 'meconfigmrg.exe' im Hauptverzeichnis der Installation von GFI MailEssentials.

2. Klicken Sie auf die Schaltfläche **Importieren**, wählen Sie den Ordner mit den exportierten Konfigurationseinstellungen von GFI MailEssentials und klicken Sie auf **OK**.

3. Klicken Sie zum Abschluss auf die Schaltfläche **Beenden**.

Importieren über die Befehlszeile

1. Stoppen Sie den Dienst IIS Admin und GFI MailEssentials Attended mit dem Befehl 'services.msc', und stoppen Sie die Dienste.

2. Öffnen Sie eine Befehlszeile, und suchen Sie nach dem Hauptinstallationsordner von GFI MailEssentials.

3. Geben Sie Folgendes ein:

```
meconfigmgr /import:”c:\MailEssentials Settings” /verbose /replace
```

Hinweis: Ersetzen Sie “C:\MailEssentials Settings” durch den gewünschten Quellpfad.

```
meconfigmgr.exe /import:"c:\MailEssentials Settings" /verbose /replace
[c:\MailEssentials Settings\config.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\config.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\autowhitelist.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\weights.bsp] wird kopiert -> [C:\Program Files\GFI\MailEssentials\Data\weights.bsp]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\userlist.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\userlist.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\pop2exchange.xml] wird kopiert -> [C:\Program Files\GFI\MailEssentials\pop2exchange.xml]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\spamord.xml] wird kopiert -> [C:\Program Files\GFI\MailEssentials\spamord.xml]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\reports.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\Data\reports.mdb]
Datei vorhanden, wurde überschrieben
==== Importieren... Fertig! ====
==== Überprüfen... ====
Anti-Spam-Aktionspfade werden überprüft...
Konfiguration der Installationspfade von GFI MailEssentials wird überprüft...
Konfiguration der Installationspfade von GFI MailEssentials wird überprüft... Fertig!
==== Überprüfen... Fertig! ====

Fertig_
```

Bild 87 - Importieren von Einstellungen über die Befehlszeile

- Der Parameter **/Verbose** weist das Tool an, den Arbeitsfortschritt beim Kopieren der Dateien wie in der folgenden Abbildung anzuzeigen.
- Der Parameter **/Replace** weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.

5.5 Konfigurieren automatischer Updates

GFI MailEssentials kann so konfiguriert werden, dass automatisch nach Updates gesucht und diese heruntergeladen werden.

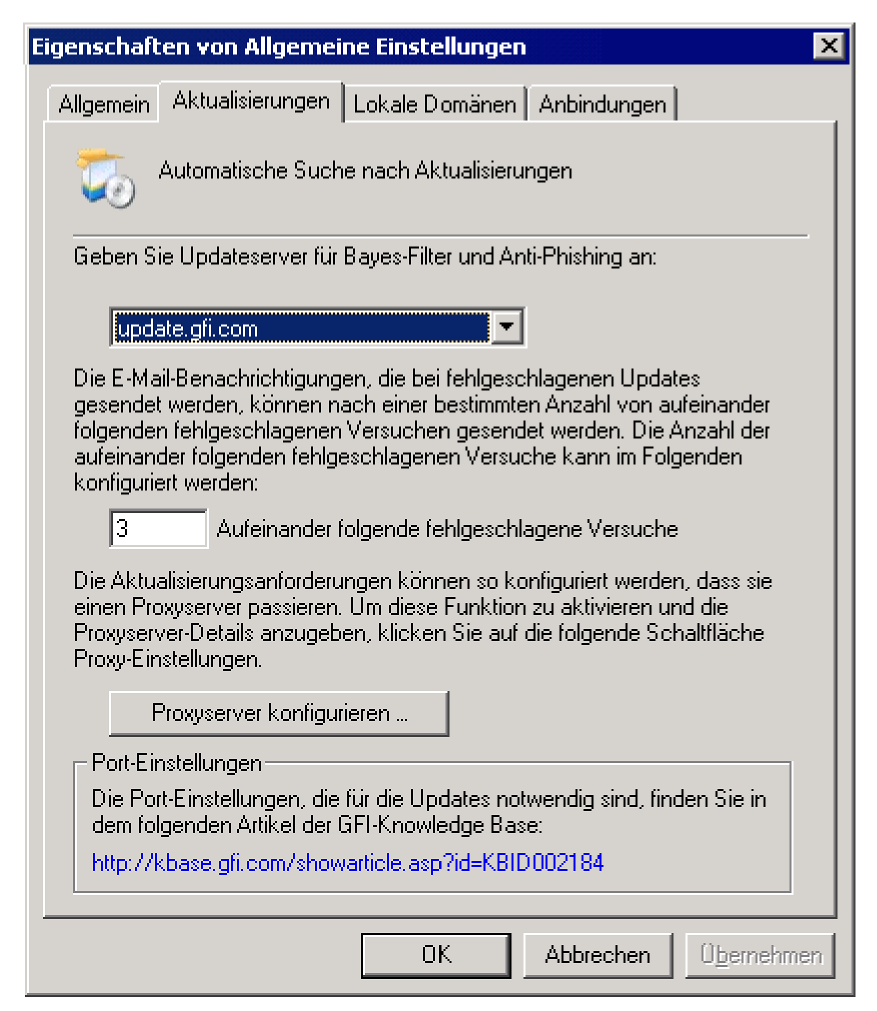


Bild 88 - Konfigurieren automatischer Updates

1. Klicken Sie zur Konfiguration automatischer Updates auf den Knoten **Allgemein ► Allgemeine Einstellungen**, klicken Sie dann auf die Registerkarte **Eigenschaften** und dann auf **Aktualisierungen**.

- Geben Sie an, auf welchen Servern nach Updates gesucht werden soll, und laden Sie Bayes-Spamfilter-Updates und Anti-Phishing-Updates herunter.
- Geben Sie an, wie oft ein Update hintereinander fehlschlagen darf, bevor eine E-Mail-Nachricht gesendet wird.
- Um Updates über einen Proxyserver herunterzuladen, klicken Sie auf **Proxyserver konfigurieren …** . Geben Sie in dem Dialog "Proxy-Einstellungen" die Einstellungen für den Proxyserver an.

2. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

5.6 Auswahl des virtuellen SMTP-Servers zur Bindung an GFI MailEssentials

Bei mehreren virtuellen SMTP-Servern müssen Sie gegebenenfalls GFI MailEssentials an neue oder andere virtuelle SMTP-Server anbinden.

HINWEIS: Die Registerkarte Virtuelle SMTP-Server-**Anbindungen** wird nicht angezeigt, wenn Sie GFI MailEssentials auf einen Computer mit Microsoft Exchance Server 2007/2010 installiert haben.

5.6.1 Anbindungen von GFI MailEssentials an virtuelle SMTP-Server

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Allgemein ► Allgemein Einstellungen**, dann auf **Eigenschaften** und die Registerkarte **Anbindungen**.

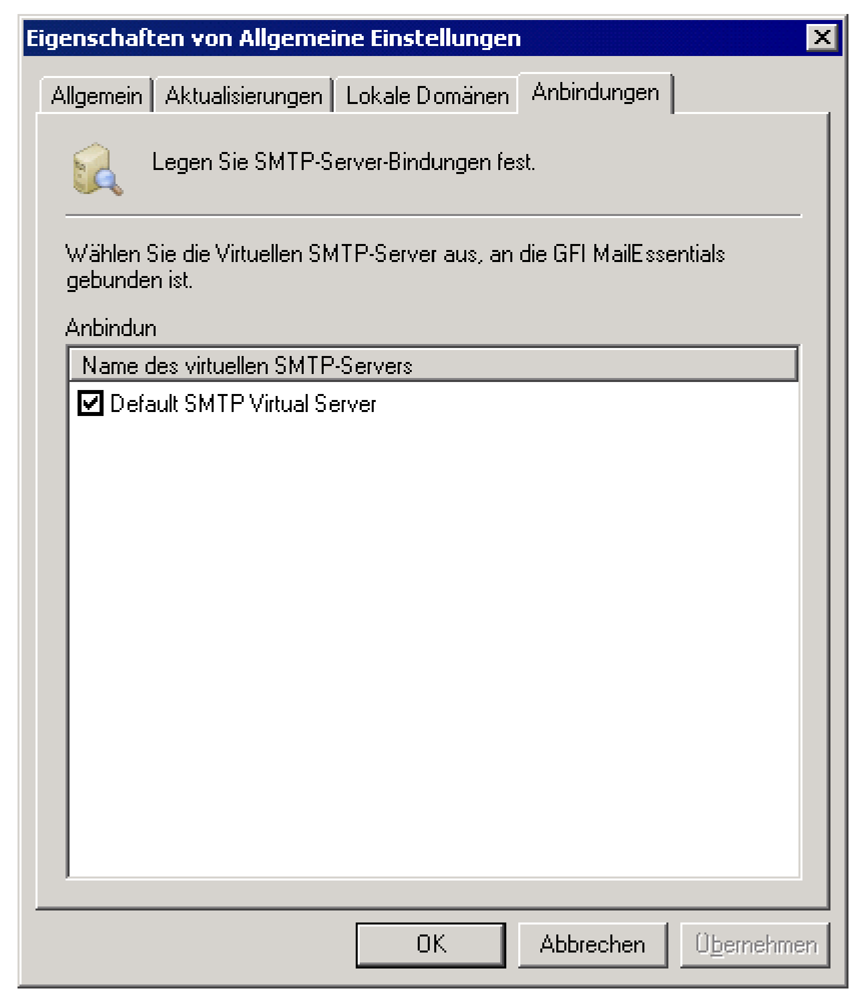


Bild 89 - Anbindungen für den virtuellen SMTP-Server

2. Klicken Sie in der Liste **Name des virtuellen SMTP-Servers** in das Kontrollkästchen des virtuellen SMTP-Servers um die Anbindung mit GFI MailEssentials herzustellen.

3. Klicken Sie auf die Schaltfläche **OK** um die Konfiguration zu übernehmen.

HINWEIS: Die Konfiguration von GFI MailEssentials verlangt einen Neustart der Dienste wie beispielsweise des IIS SMTP-Dienstes, damit die neuen Einstellungen wirksam werden. Klicken Sie auf die Schaltfläche **Ja** um die Dienste neu zu starten.

5.7 Remote-Befehle

Remote-Befehle erleichtern das Hinzufügen von Domänen oder E-Mail-Adressen zur Spam-Blacklist sowie eine Aktualisierung des Bayes-Filters SPAM oder HAM (zulässigen E-Mails).

Remote-Befehle senden eine E-Mail an GFI MailEssentials. Wenn Sie

eine E-Mail an rcommands@mailessentials.com (konfigurierbar) senden, erkennt GFI MailEssentials, dass die E-Mail Remote-Befehle enthält und verarbeitet die Befehle.

Mit Remote-Befehlen können Sie folgende Aufgaben ausführen:

1. Sie können SPAM oder HAM für das Bayes-Modul hinzufügen.

2. Sie können entweder Keywords für die Prüfung der Betreffzeile oder des Nachrichtentextes hinzufügen.

3. Sie können E-Mail-Adressen zum Blacklist-Filter hinzufügen.

5.7.1 Konfigurieren von Remote-Befehlen

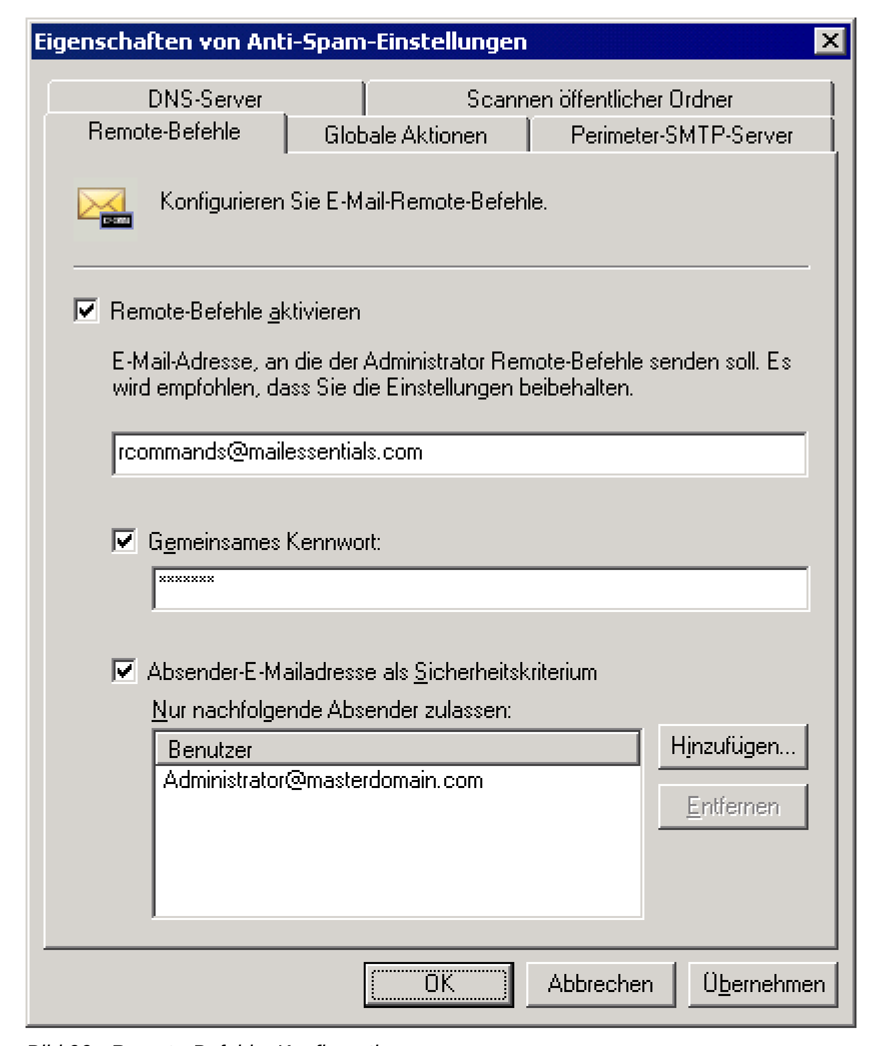


Bild 90 - Remote-Befehle, Konfiguration

1. Klicken Sie mit der rechten Maustaste auf **Anti-Spam ► Anti-Spam-Einstellungen**, dann auf **Eigenschaften**, klicken Sie auf die Registerkarte **Remote-Befehle** und dann in das Kontrollkästchen **Remote-Befehle aktivieren**.

2. Bearbeiten Sie die E-Mail-Adresse, an die die Remote-Befehle gesendet werden sollen.

HINWEIS: Die E-Mail-Adresse sollte keine lokale Domäne sein. Wir empfehlen als Adresse rcommands@mailessentials.com. Ein Postfach für die konfigurierte Adresse muss nicht existieren, aber der Domänenteil der Adresse muss mit einer real existierenden E-Mail-

Adressen-Domäne übereinstimmen, die bei einer MX-Eintragssuche über DNS ein positives Ergebnis liefert.

3. Optional können Sie einige Basissicherheitsfunktionen für Remote-Befehle konfigurieren:

- Konfigurieren Sie ein gemeinsames Kennwort, das in der E-Mail enthalten sein soll. Weitere Informationen finden Sie unter Verwendung von Remote-Befehlen in diesem Handbuch.
- Konfigurieren Sie außerdem, welche Benutzer E-Mails mit Remote-Befehlen versenden dürfen.

HINWEIS: Die Benutzer können diese Einschränkungen umgehen, indem sie die Absenderadresse fälschen.

Kennwörter werden als separate Befehle mit folgender Syntax versendet:

KENNWORT: <gemeinsames Kennwort>;

5.7.2 Verwendung von Remote-Befehlen

Die Remote-Befehle müssen folgende Syntax besitzen:

<command>: <param1>, [<param2>, <param3>, …];

Im Text einer E-Mail darf mehr als ein Befehl enthalten sein, wenn die einzelnen Befehle mit einem Semikolon getrennt sind (;). Jeder Befehlsname unterscheidet zwischen Groß- und Kleinschreibung und sollte in Großbuchstaben geschrieben sein. Folgende Befehle sind verfügbar:

HINWEIS: Der Roboter kann nur Keywords hinzufügen, diese aber nicht löschen oder verändern. Bedingungen werden nicht unterstützt.

Verfügbare Befehle sind:

- **ADDSUBJECT** - Ergänzt Keywords für die Datenbank, die die Keywords in der Betreffzeile prüft.
  - **Beispiel:** ADDSUBJECT: sex, porn, spam;
- **ADDBODY** - Ergänzt Keywords in der Datenbank, die nach Keywords im Nachrichtentext sucht.
  - **Beispiel:** ADDBODY: free, “100% free”, “absolutely free”;

HINWEIS: Wenn Sie Phrasen konfigurieren, die aus mehreren Wörtern bestehen, schließen Sie die Phrasen in doppelte Anführungszeichen ein (“ ”).

5.7.3 Blacklist-Befehle

Mit Blacklist-Befehlen ergänzen Sie eine einzelne E-Mail-Adresse oder eine komplette Domäne in der benutzerdefinierten Blacklist.

Verfügbare Befehle sind:

- **ADDBLIST:** <email>;
  - **Beispiel:** ADDBLIST: user@somewhere.com;

HINWEIS 1: Fügen Sie eine komplette Domäne in der Blacklist hinzu, indem Sie ein Ersatzzeichen vor der Domäne einfügen

- **Beispiel:** ADDBLIST: *@Domäne.com.

HINWEIS 2: Aus Sicherheitsgründen darf nur ein Befehl ADDBLIST in

einer E-Mail enthalten sein, und es darf nur eine Adresse als Befehlsparameter angegeben sein. Der Parameter ist entweder eine Benutzer-E-Mail oder eine Domäne:

- **Beispiel:** spammer@spam.com oder *@spammers.org.

HINWEIS 3: Ersatzzeichen können in Domänennamen nicht verwendet werden.

- **Beispiel:** *@*.domäne.com wird als ungültig zurückgewiesen.

5.7.4 Bayes-Filter-Befehle

Ergänzen Sie Spam-Mails oder zulässige E-Mails (HAM) in der Bayes-Filter-Datenbank. Verfügbare Befehle sind:

- **ADDASSPAM** - weist den Bayes-Filter an, die E-Mail als Spam-Mail einzustufen.
- **ADDASGOODMAIL**Weist den Bayes Bayes-Filter an, die E-Mail als HAM einzustufen.

HINWEIS: Für diese Befehle gibt es keine Parameter - der Parameter ist der Rest der E-Mail.

Beispiele

- **Beispiel 1**- Bei diesem Beispiel ergänzt der Benutzer spammer@spamhouse.com in der Blacklist und fügt einige Keywords in der Datenbank hinzu, die nach Keywords in der Betreffzeile sucht.

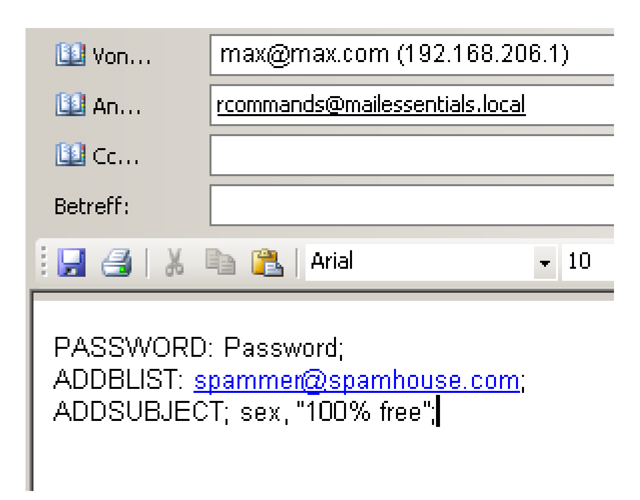


Bild 91 - Hinzufügen einer E-Mail-Adresse zur Blacklist und Keywords

- **Beispiel 2** - Der gleiche Befehl kann mehr als einmal angegeben werden (in diesem Fall ADDBODY). Das Ergebnis ist kumulativ und in diesem Fall werden folgende Keywords in der Datenbank hinzugefügt, die Keywords im Nachrichtentext prüft: sex, 100% free und instant money.

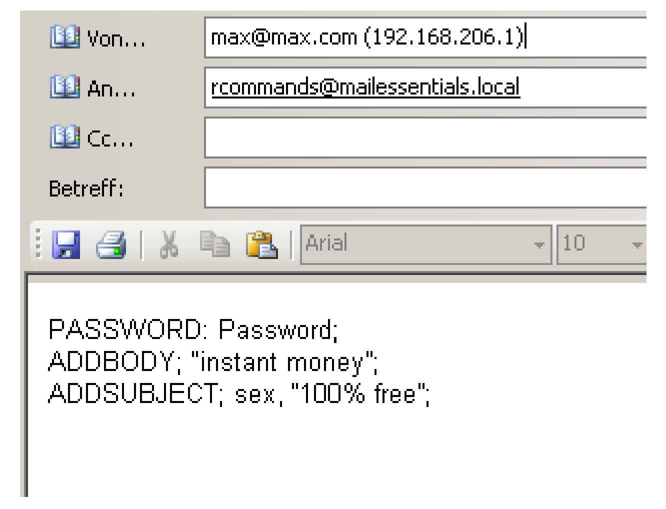


Bild 92 - Mehrmalige Definition des gleichen Befehls

- **Beispiel 3:** Eine Spam-Mail wird mit dem Befehl ADAASSPAM hinzugefügt. Bei diesem Befehl ist ein Doppelpunkt nicht erforderlich - alles unmittelbar nach diesem Befehl wird als Daten behandelt.

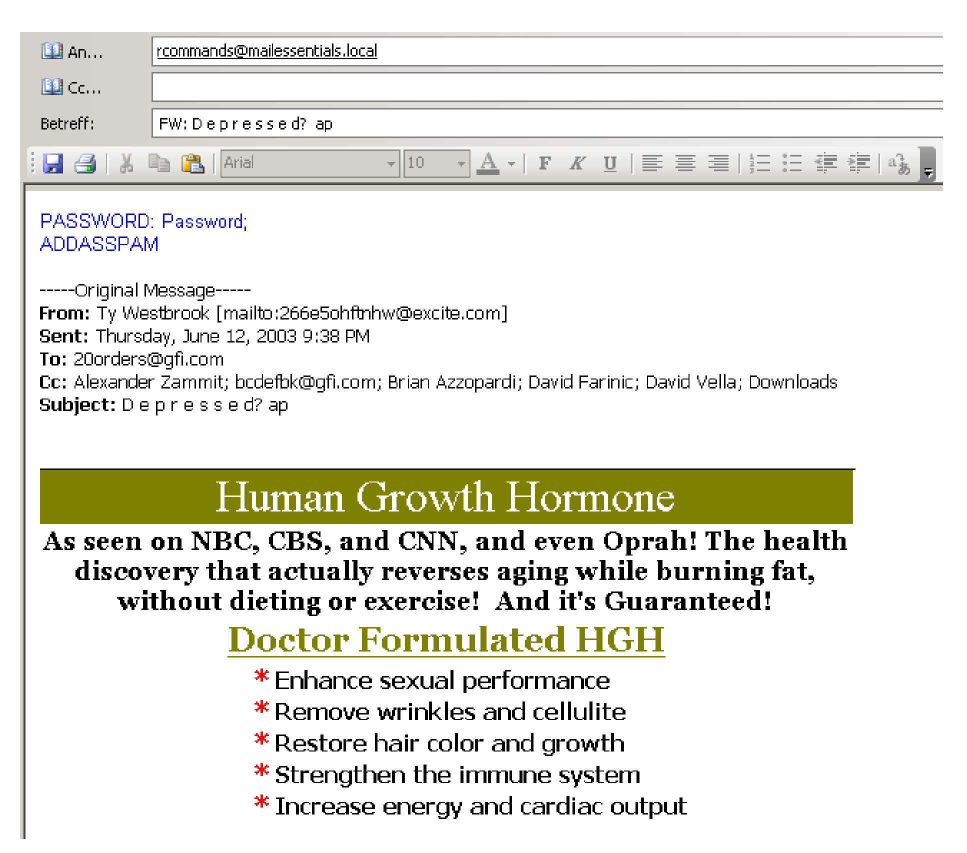


Bild 93 - Hinzufügen von Spam-Mails in der Bayes-Filterdatenbank

- **Beispiel 4** - Wenn das Kontrollkästchen **Gemeinsames Kennwort** nicht aktiviert ist, können Remote-Befehle ohne Kennwort gesendet werden.

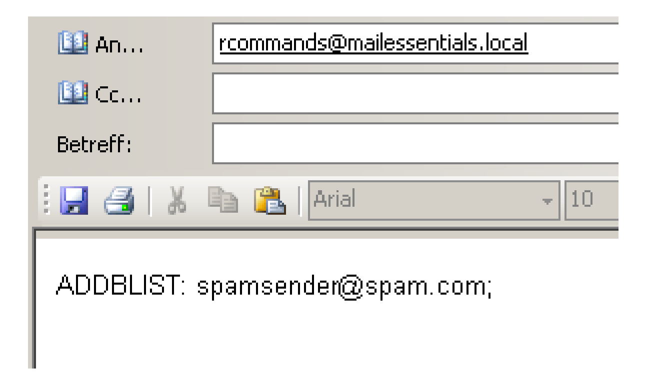


Bild 94 - Senden von Remote-Befehlen ohne Sicherheit

5.7.5 Protokollieren von Remote-Befehlen

Damit Änderungen an der Konfigurationsdatenbank, die über Remote-Befehle vorgenommen wurden, verfolgt werden können, wird jede E-Mail, die mit Remote-Befehlen (selbst wenn die E-Mail mit den Remote-Befehlen ungültig war) in dem Unterordner ADBRProcessed in dem Hauptordner von GFI MailEssentials gespeichert. Der Dateiname in jeder E-Mail wird entsprechend folgendem Format formatiert:

- **<Absender_E-Mail_Adresse>_SUCCESS_<Zeitstempel>.eml** - bei einer erfolgreichen Bearbeitung.
- **<Absender_E-Mail_Adresse>_FAILED_<Zeitstempel>.eml** - bei einem Fehler.

HINWEIS: Der Zeitstempel wird formatiert als yyyyddmmhhmmss.

5.8 Verschieben von Spam-E-Mails in den Postfachordner des Benutzers

Wenn GFI MailEssentials auf einem Microsoft Exchange Server installiert ist, speichern Sie Spam-E-Mails entsprechend der Beschreibung im Kapitel Spam-Aktionen - Umgang mit Spam-Mails auf Seite 78 in diesem Handbuch.

Wenn GFI MailEssentials NICHT auf einem Microsoft Exchange Server installiert ist, können Spam-E-Mails nicht mit der Option "Spam-Aktionen" in einen spezifischen Postfachordner des Benutzers umgeleitet werden. Die E-Mails können jedoch wie im Folgenden beschrieben in das Postfach des Benutzers umgeleitet werden.

5.8.1 Microsoft Exchange Server 2000/2003

GFI MailEssentials enthält einen Regelmanager, der als Spam gekennzeichnete E-Mails automatisch in das Benutzerpostfach verschiebt.

HINWEIS: Der Rules Manager läuft nur unter Windows 2000 oder höher.

WICHTIGER HINWEIS: Um den Rules Manager zu verwenden, klicken Sie unter **Spam-Aktionen auf die Option "E-Mail mit bestimmtem Text markieren**" und geben einen Kennzeichnungstext an.

Rules Manager auf Microsoft Exchange Server installieren

1. Suchen Sie auf dem Computer mit GFI MailEssentials den Installationsordner von GFI MailEssentials.

2. Kopieren Sie die folgenden Dateien in einen Ordner auf dem Microsoft Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. Öffnen Sie auf Microsoft Exchange Server eine Befehlszeile und ändern Sie das Verzeichnis für den Speicherort, in den die Dateien des Rules Manager kopiert wurden.

4. Geben Sie auf der Befehlszeile Folgendes ein: **regsvr32 rule.dll**

5. Klicken Sie zur Bestätigung auf **OK** .

Rules Manager starten

1. Suchen Sie auf dem Microsoft Exchange Server den Ort, an den die Dateien des Rules Manager kopiert wurden und öffnen Sie die Datei **rulemgmt.exe**..

2. Wählen Sie eine Microsoft Outlook Profildatei (MAPI-Profil) aus oder erstellen Sie ein neues Profil für die Anmeldung (nur, wenn Sie den Rules Manager erstmals verwenden).

3. Klicken Sie auf **OK**, um den Rules Manager zu starten.

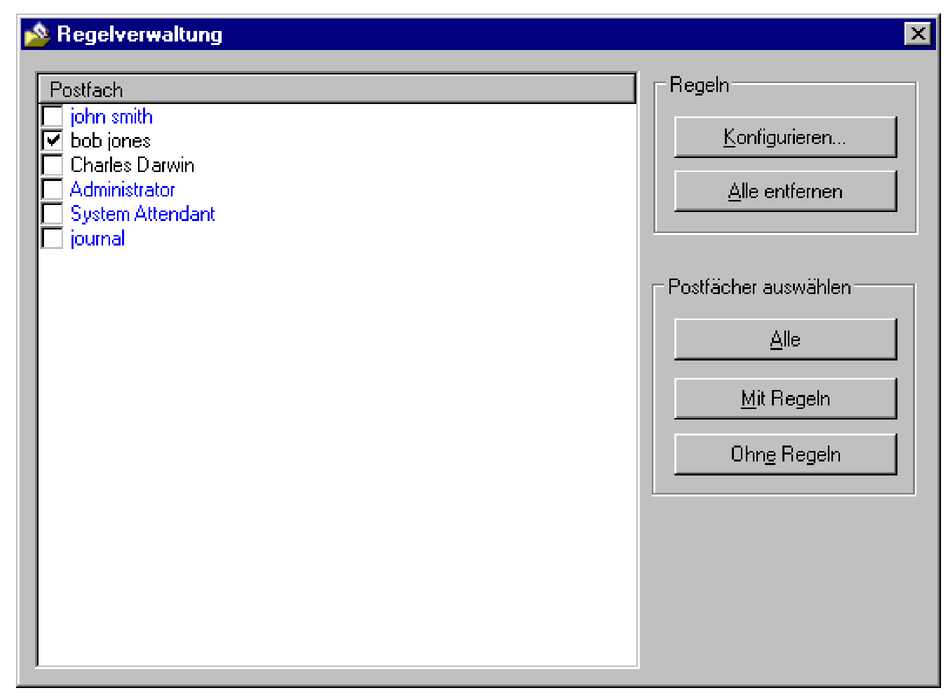


Bild 95 - Der Rules Manager von GFI MailEssentials

4. Das Hauptfenster des Rules Manager zeigt alle auf dem Microsoft Exchange Server aktivierten Postfächer. Die Farbe der Postfächer gibt den Status des betreffenden Postfachs an:

- Blau - Postfach mit konfigurierten Regeln

- Schwarz - Postfach ohne konfigurierte Regeln

Definieren neuer Regeln

1. Markieren Sie die Postfächer, für die Sie eine Regel definieren wollen und klicken Sie auf **Konfigurieren …**, um den Dialog **Globale Regel konfigurieren** zu starten.

HINWEIS 1: Sie können neue Regeln zu Postfächern hinzufügen, die bereits Regeln enthalten.

HINWEIS 2: Wählen Sie mehrere Postfächer aus, um die gleiche Regel für alle Postfächer zu konfigurieren -



Bild 96 - Hinzufügen einer neuen Regel im Rules Manager

2. Geben Sie in dem Textfeld **Regelbedingung** die Kennzeichnung ein, die die Spam-E-Mail durch die Option "Spam-Aktionen" von GFI MailEssentials erhält.

3. Geben Sie die **Regelaktion** ein:

- Klicken Sie auf **Löschen**, um die E-Mail zu löschen, deren Betreff die Regelbedingung enthält.
- Klicken Sie auf **Verschieben in:** , Um eine Spam-E-Mail in einen Ordner des Postfachs zu verschieben. Geben Sie den Ordnerpfad ein, in den die Spam-E-Mail verschoben werden soll. Wenn Sie "**Posteingang\Spam**" angeben, wird ein Spamordner im Posteingangsordner erstellt. Wenn Sie nur "**Spam**" eingeben, wird der Ordner auf der obersten Ebene (gleiche Ebene wie Posteingang) erstellt.

4. Klicken Sie auf **Übernehmen**, um die definierten Regeln zu speichern.

Verwalten mehrerer Regeln

Sie können für das gleiche Postfach mehr als eine Regel definieren.

Beispiel: Mit [Phishing] markierte E-Mails löschen und mit [Spam] gekennzeichnete E-Mails in den Posteingangs-Spamordner verschieben.

1. Doppelklicken Sie auf ein Postfach, um den Regeldialog zu starten.

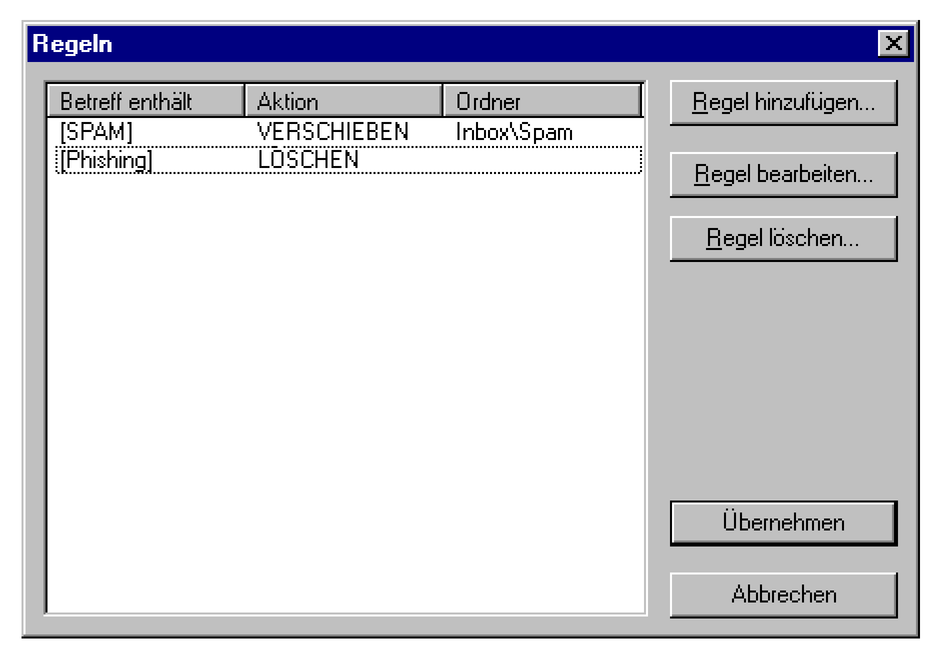


Bild 97 - Liste der Regeln in Rules Manager

2. Es wird eine Liste der für den ausgewählten Posteingang geltenden Regeln angezeigt.

- Klicken Sie auf **Regel hinzufügen**, um eine neue Regel hinzuzufügen.
- Wählen Sie eine Regel aus und klicken Sie auf **Regel bearbeiten**, um die Einstellungen für die ausgewählte Regel zu ändern.
- Wählen Sie ein Regel aus und klicken Sie auf **Regel löschen**, um die ausgewählte Regel zu löschen.

3. Klicken Sie auf **&Übernehmen**, um die Einstellung zu speichern.

5.8.2 Microsoft Exchange 2007/2010

Um Microsoft Exchange 2007/2010 so zu konfigurieren, dass gekennzeichnete E-Mails in den Junk-Postfachordner des Benutzers weitergeleitet werden, müssen Sie eine Transportregel erstellen.

WICHTIGER HINWEIS: Klicken Sie in GFI MailEssentials "Spam-Aktionen" auf die Option **E-Mail mit bestimmtem Text kennzeichnen** . Wenn Sie auf eine andere Aktion klicken, erreichen die als Spam erkannten E-Mails nicht das Postfach des Benutzers, und daher bleiben die konfigurierten Transportregeln unwirksam.

So erstellen Sie eine Transportregel in Exchange 2007/2010:

1. Starten Sie die **Microsoft Exchange Managementkonsole**.

2 Wechseln Sie zum Knoten **Microsoft Exchange ► Organisationskonfiguration ► Hub-Übertragung** und klicken Sie auf die Option **Übertragungsregeln**.

3. Klicken Sie zum Start des Assistenten auf **Neue Transportregel**.

4. Geben Sie für die neue Regel einen Namen ein (beispielsweise GFI MailEssentials Spam) und klicken Sie auf **Weiter** .

5. Wählen Sie in dem Bereich **Bedingungen** die Option **Wenn das Betrefffeld bestimmte Worte enthält aus**.

6. Klicken Sie in dem Bereich **Regel bearbeiten** auf **bestimmte Worte**, um die für die Kennzeichnung verwendeten Worte einzugeben. Geben Sie die in den unter "Spam-Aktionen" definierten Kennzeichnungen für jeden Spamfilter ein und klicken Sie auf **Hinzufügen** (Beispiel: [SPAM]). Klicken Sie auf **OK**, wenn alle Worte hinzugefügt sind und dann auf **Weite**r .

7. Klicken Sie im Bereich "Aktionen" auf die Option **Spam-Konfidenzgrad auf Wert setzen** .

8. Klicken Sie im Bereich **Regel bearbeiten** auf **0** und setzen Sie den Konfidenzgrad auf **9**. Klicken Sie auf **OK** und dann auf **Weiter** .

9. (Optional) Definieren Sie Ausnahmen für diese Transportregeln und klicken Sie dann auf **Weiter** .

10. Klicken Sie auf **Neu**, um eine neue Transportregel zu erstellen.

HINWEIS: Achten Sie darauf, dass der Junk-E-Mail-Ordner für die Benutzerpostfächer aktiviert ist.

Die erstellte Transportregel leitet jetzt alle E-Mails, die die Kennzeichnung von GFI MailEssentials enthalten, in den Junk-E-Mail-Ordner der Benutzer.

5.9 Rückverfolgung

GFI MailEssentials kann Protokolle zur Fehlerbehebung erstellen. Ist diese Option aktiviert, speichert GFI MailEssentials die Aktivitäten in dem Ordner "DebugLogs" im Installationsordner von GFI MailEssentials. So konfigurieren Sie die Rückverfolgung:

1. Klicken Sie auf **Start ► Programme ► GFI MailEssentials ► GFI MailEssentials Switchboard.**

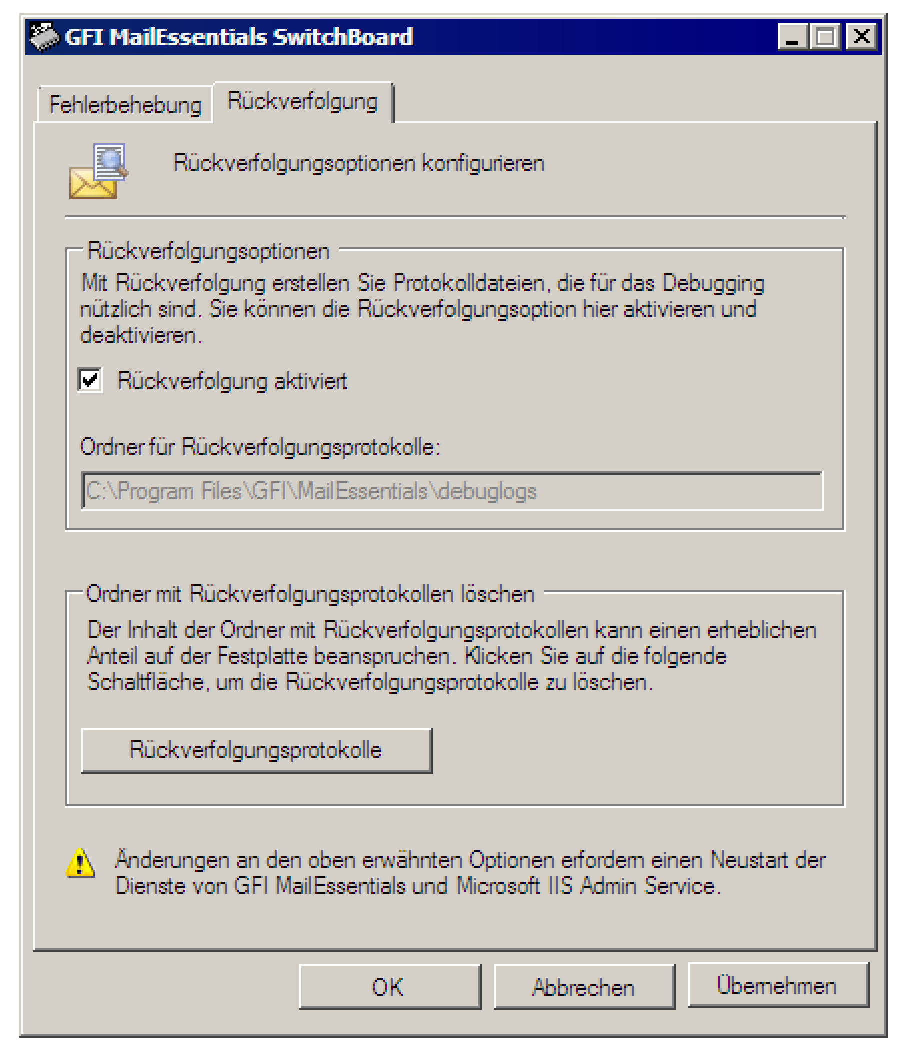


Bild 98 - Rückverfolgung

2. Klicken Sie auf die Registerkarte **Rückverfolgung** und konfigurieren Sie folgende Optionen:

- Markieren oder demarkieren Sie das Kontrollkästchen **Rückverfolgung aktiviert**, um die Rückverfolgung zu aktivieren oder zu deaktivieren. Diese Option ist standardmäßig aktiviert.
- Klicken **Rückverfolgungsprotokolle**, um alle Protokolle zu löschen.

E-Mail-Sicherung vor/nach der Verarbeitung

WICHTIGER HINWEIS: Wir empfehlen unbedingt, diese Option deaktiviert zu lassen und nur für die Fehlerbehebung nach Anleitung von Fachpersonal zu verwenden.

Markieren/demarkieren Sie das **Kontrollkästchen "Eine Kopie jeder E-Mail vor und nach der E-Mail-Verarbeitung behalten**", um eine Kopie jeder verarbeiteten E-Mail in dem Ordner "SinkArchives" im Installationsordner von GFI MailEssentials.

6 Problembehandlung & Support

6.1 Einführung

Dieses Kapitel erläutert, wie Probleme bei der Installation von GFI MailEssentials beseitigt werden können. Nutzen Sie die folgenden Informationsquellen in der im Folgenden aufgelisteten Reihenfolge:

1. Dieses Handbuch
2. Die Abschnitte "Häufige Probleme" im Folgenden
3. Die Artikel in der GFI Knowledge Base
4. Gemeinsame Prüfungen
5. Web-Foren
6. Kontakt zum technischen Support von GFI

6.2 Benutzerhandbuch

Nutzen Sie die Informationen in diesem Benutzerhandbuch um zu erkennen, welche Ursachen Probleme bei der Installation von GFI MailEssentials haben könnten. Die Informationskapitel sowie die Kapitel Häufige Probleme enthalten Anleitungen, wie Sie Probleme beseitigen können, die aufgrund menschlicher Fehler oder aufgrund von Fehlkonfigurationen auftreten.

6.3 Häufige Probleme

Die Liste häufiger Probleme im Folgenden enthält Probleme, die andere Benutzer häufiger bei der Nutzung von GFI MailEssentials festgestellt haben.

6.3.1 Umgang mit Spam

Festgestelltes Problem	Lösung
1. Das Dashboard zeigt, dass keine E-Mail verarbeitet wird: Es werden nur eingehende oder nur ausgehende E-Mails verarbeitet.	1. Kontrollieren Sie, dass das Scannen von E-Mails durch GFI MailEssentials nicht deaktiviert wurde. Weitere Informationen, wie Sie den Scan-Vorgang starten, finden Sie in Kapitel Deaktivieren/Aktivieren des Scannens von E-Mail in diesem Handbuch. 2. Kontrollieren Sie, ob mehrere virtuelle Microsoft IIS SMTP-Server IIS SMTP vorhanden sind, und ob GFI MailEssentials an den richtigen virtuellen Server gebunden ist. 3. MX-Eintrag für die Domäne nicht richtig konfiguriert. Kontrollieren Sie, ob der MX-Eintrag auf die IP-Adresse des Servers zeigt, auf dem GFI MailEssentials gestartet ist. 4. Wenn eingehende E-Mails durch ein anderes Gateway laufen, kontrollieren Sie, ob der Mail-Server auf dem anderen Gateway eingehende E-Mails über GFI MailEssentials weiterleitet. 5. Achten Sie darauf, dass ausgehende E-Mails so konfiguriert sind, dass sie über GFI MailEssentials geleitet werden. Weitere Details finden Sie im Installationshandbuch. 6. Überprüfen Sie, ob der virtuelle SMTP-Server von Microsoft Exchange Server für ausgehende E-Mails der gleiche SMTP-Server ist, an den GFI MailEssentials gebunden ist. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003286
2. Nach der Installation von GFI MailEssentials zeigen einige E-Mails im Nachrichtentext Garbage an, wenn sie im GFI MailArchiver oder in Microsoft Outlook betrachtet werden.	Dieses Problem tritt bei E-Mails auf, bei denen ein bestimmter Zeichensatz im Nachrichten-Header definiert ist und ein anderer Zeichensatz für den Nachrichtentext. Wenn solche E-Mails von Microsoft Exchange 2003 bearbeitet werden, werden die E-Mails in Microsoft Outlook und GFI MailArchiver als Garbage angezeigt. Microsoft hat ein Hotfix freigegeben um dieses Problem zu beseitigen. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003459 und http://support.microsoft.com/kb/916299

6.3.2 Archivierung und Berichterstellung

Festgestelltes Problem	Lösung
1. Als Spam gekennzeichnete E-Mails werden archiviert.	1. Starten Sie den Regeln-Manager auf dem Computer mit Microsoft Exchange, indem Sie auf 'rulemgmt.exe' im Ordner von GFI MailEssentials doppelklicken. 2. Aktivieren Sie das Kontrollkästchen neben dem Namen des Postfachs, das von GFI MailArchiver zur Archivierung abgefragt wird. 3. Klicken Sie auf **Konfigurieren** und achten Sie darauf, dass die Einstellungen der 'Regelbedingungen' und die 'Regelaktion' korrekt sind. Klicken Sie auf **Übernehmen**. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002747
2. AWI kann nicht erreicht werden. Meldung "HTTP Error 404 - Datei oder Verzeichnis nicht gefunden".	Standardmäßig deaktiviert Internet Information Services (IIS) dynamischen Content. Für AWI muss dynamischer Content aktiviert sein, da die Daten dynamisch aus der Archivdatenbank geladen werden. 1. Laden Sie IIS Manager, öffnen Sie den Knoten ***<Servername>***

	► Webserviceerweiterungen und klicken Sie mit der rechten Maustaste auf 'Active Server Pages'. 2. Klicken Sie auf **Zulassen** um den Status auf 'Zugelassen' zu ändern. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002963
3. Ältere Daten sind in der Datenbank bei Verwendung von Microsoft Access nicht verfügbar.	Wenn die Datenbank-Reports.mdb größer als 1,7 GB wird, wird die Datenbank automatisch umbenannt in *reports_data.mdb* und es wird eine neue Datenbank reports.mdb erstellt. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003422

6.3.3 Spam-Filter und Spam-Aktionen

Festgestelltes Problem	Lösung
1. Spam-Nachrichten gelangen in das Postfach der Benutzer.	Arbeiten Sie die folgende Checkliste ab um dieses Problem zu beheben: 1. Überprüfen Sie, dass das Scannen von E-Mails mit GFI MailEssentials nicht deaktiviert ist. Weitere Informationen zum Start des Scan-Vorgangs finden Sie im Abschnitt Deaktivieren/Aktivieren des Scannens von E-Mail in diesem Handbuch. 2. Prüfen Sie, ob alle benötigten Spam-Filter aktiviert sind. 3. Prüfen Sie, ob lokale Domänen korrekt konfiguriert sind. 4. Prüfen Sie, ob die E-Mails GFI MailEssentials passieren bzw. ob GFI MailEssentials an den richtigen virtuellen IIS SMTP-Server IIS SMTP gebunden ist. 5. Prüfen Sie, ob der Speicherort '%TEMP%' (standardmäßig im Ordner C:\Windows\Temp') viele Dateien enthält. 6. Prüfen Sie, ob die Anzahl der Benutzer, die GFI MailEssentials nutzen, größer ist als die Zahl der gekauften Lizenzen. 7. Prüfen Sie, ob die Whitelist korrekt konfiguriert ist. 8. Prüfen Sie, ob die Aktionen korrekt konfiguriert sind. 9. Prüfen Sie, ob der Bayes-Filter Bayes korrekt konfiguriert ist. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003256
2. Benutzerdefinierte Blacklists bzw. Seiten zur Keyword-Prüfung benötigen viel Zeit oder hängen sich auf.	Begrenzen Sie die Anzahl der Einträge in den Listen von GFI MailEssentials auf 10.000. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002915 und: http://kbase.gfi.com/showarticle.asp?id=KBID003267
3. SpamRazer-Aktualisierungen werden nicht heruntergeladen.	1. Prüfen Sie, ob Ihr Lizenzschlüssel gültig ist. 2. Achten Sie darauf, dass die benötigten Ports geöffnet sind, und dass Ihre Firewall-Verbindungen von GFI MailEssentials-Server zu einem Proxy-Server entsprechend der Definition in Ihrer Konfiguration zulässt. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002184

6.3.4 Haftungsausschluss

Festgestelltes Problem	Lösung
1. Es werden keine Haftungsausschlüsse bei ausgehenden Mails ergänzt.	Prüfen Sie, ob die lokalen Domänen richtig konfiguriert sind. Weitere Informationen finden Sie in der Kurzanleitung.
2. Einige Zeichen im Text des Haftungsausschlusses werden nicht richtig angezeigt.	Konfigurieren Sie Microsoft Outlook so, dass die automatische Codierung nicht verwendet wird, und erzwingen Sie eine korrekte Codierung für GPO. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://office.microsoft.com/en-us/ork2003/HA011402641033.aspx
3. Der Haftungsausschluss wird selbst dann versendet, wenn er deaktiviert ist.	Starten Sie GFI MailEssentials und IIS Services neu, nachdem Sie einen Haftungsausschluss deaktiviert haben, damit die Änderungen wirksam werden.

6.3.5 E-Mail-Überwachung

Festgestelltes Problem	Lösung
1. E-Mails, die von bestimmten Benutzern versendet werden oder an bestimmte Benutzer gesendet werden, werden nicht überwacht.	Die Regeln zur E-Mail-Überwachung überwachen weder die E-Mails vom bzw. an den Administrator von GFI MailEssentials noch die E-Mail-Adresse, an die die überwachten E-Mails gesendet werden. Regeln zur E-Mail-Überwachung sind auch dann nicht verfügbar, wenn es sich um E-Mails zwischen internen Benutzern des gleichen Informationsdienstes handelt.

6.3.6 Listenserver

Festgestelltes Problem	Lösung
1. E-Mails, die an den Listenserver gesendet werden, werden nur in Textformat konvertiert.	E-Mails, die an den Listenserver gesendet werden, werden nur in Textformat konvertiert, wenn das Originalformat der E-Mail RTF-Format war. Im HTML-Format versendete E-Mails behalten das Originalformat.
2. Interne Benutzer erhalten einen Unzustellbarkeitsbericht, wenn sie E-Mails an einen Listenserver senden und GFI MailEssentials auf einem Gateway installiert ist.	Weitere Informationen zur Verwendung der Listenserverfunktion bei Installation von GFI MailEssentials finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002123

6.3.7 Verschiedenes

Festgestelltes Problem	Lösung
1. Das Dashboard meldet den Fehler "Ungültiger Benutzer oder Kennwortfehler beim Verbindungsaufbau mit dem POP3-Server..." fehler	Überprüfen Sie, ob Microsoft Exchange Information Store gestartet ist. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID001805
2. Mit Microsoft Exchange über POP3 verbundene Clients können als Spam gekennzeichnete E-Mails nicht sehen.	Stellen Sie die Verbindung mit Microsoft Exchange über IMAP her. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002644
3. Automatische Aktualisierungen schlagen fehl, das manuelle Herunterladen über die Konfiguration von GFI MailEssentials funktioniert jedoch einwandfrei.	Kontrollieren Sie, ob nicht authentifizierte Verbindungen von den Computern mit GFI MailEssentials an http//update.gfi.com auf Port 80 zugelassen werden. Weitere Informationen zur Beseitigung des Problems finden Sie

	unter: http://kbase.gfi.com/showarticle.asp?id=KBID002116
4. Die Konfigurationsdaten können nicht importiert werden.	Kontrollieren Sie, ob die Version von GFI MailEssentials und die Build-Nummer sowohl bei der Ziel- als auch bei der Ausgangsinstallation identisch sind. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003182
5. Remote-Befehle funktionieren nicht.	Informationen zur Behebung dieses Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID001806

6.4 Knowledge Base

GFI pflegt eine umfassende Wissensdatenbank, die Antworten auf häufige Benutzerprobleme enthält.

Wenn die Informationen in diesem Handbuch nicht ausreichen um Ihre Installationsprobleme zu lösen, schlagen Sie bitte in der Knowledge Base nach. Die Knowledge Base enthält die aktuellste Liste der Fragen an den technischen Support und die aktuellen Patches. Aufrufen können Sie die Knowledge Base über:

http://kbase.gfi.com/

6.5 Gemeinsame Prüfungen

Wenn die Informationen in diesem Handbuch und in der Knowledge Base nicht ausreichen, Ihre Probleme zu beheben:

1. Kontrollieren Sie, ob Sie alle Service Packs für Ihr Betriebssystem sowie für den MailServer und GFI MailEssentials installiert haben.

2. Installieren Sie Microsoft Data Access Components (MDAC) neu um die einwandfreie Funktion sicherzustellen.

6.6 Web-Forum

Technischer Support der Benutzer untereinander ist über das GFI Web-Forum verfügbar. Schlagen Sie immer zuerst im Benutzerhandbuch und in der Knowledge Base nach, und wenden Sie sich dann an das Webforum unter:

http://forums.gfi.com/.

6.7 Anforderung von technischem Support

Wenn Sie mit keiner der oben angegebenen Ressourcen Ihre Probleme beheben können, wenden Sie sich bitte an das technische Supportteam von GFI. Füllen Sie dazu ein Online-Support-Formular aus, oder rufen Sie an.

- **Online:** Füllen Sie das Online-Supportformular aus, und folgen Sie den Anweisungen auf dieser Seite genau um Ihre Supportanforderung abzusenden: http://support.gfi.com/supportrequestform.asp.
- **Telefonischer Support:** Die korrekte Telefonnummer für den technischen Support Ihrer Region finden Sie unter: http://www.gfi.com/company/contact.htm.

HINWEIS: Halten Sie Ihre Kunden-ID bereit, bevor Sie Kontakt mit dem technischen Support von GFI aufnehmen. Ihre Kunden-ID ist die Online-Kontonummer, die Ihnen zugewiesen wurde, als Sie Ihren Lizenzschlüssel in Ihrem Kundenbereich erstmals registrierten:

http://customers.gfi.com.

GFI bemüht sich, Ihre Anfrage innerhalb von maximal 24 Stunden zu beantworten, je nach Ihrer Zeitzone.

6.8 Benachrichtigungen über Builds

Wir empfehlen Ihnen, die Liste der Build-Benachrichtigungen zu abonnieren, sodass Sie laufend über neue Produkt-Builds informiert werden. Abonnieren Sie unsere Build-Benachrichtigungen unter: http://www.gfi.com/pages/productmailing.htm

6.9 Dokumentation

Wenn dieses Handbuch Ihren Erwartungen nicht entspricht oder Sie der Meinung sind, dass die Dokumentation verbessert werden kann, senden Sie uns bitte eine E-Mail an:

documentation@gfi.com

7 Anhang 1 - Wie funktionieren Spam-Filter?

7.1 Filtern eingehender E-Mails

Das Filtern eingehender E-Mails ist ein Vorgang, bei dem eingehende E-Mails vor der Zustellung an die Benutzer analysiert werden.

1. Nach Aufbau einer Verbindung wird die Empfänger-E-Mail-Adresse der eingehenden Mail geprüft; wenn sie nicht gefunden wird, wird die Verbindung sofort beendet. Zuständig dafür ist der Directory Harvesting-Filter. Wenn die Empfänger-E-Mail-Adresse gefunden wird, erfolgt eine weitere Prüfung in der nächsten Stufe.

2. Die E-Mail wird auf Adressierung an einen Listenserver geprüft. Ist dies der Fall, wird die E-Mail an den Listenserver weitergeleitet, anderenfalls wird sie in der nächsten Stufe nochmals geprüft.

3. Die eingehende E-Mail wird durch alle Spam-Filter gefiltert. Jede E-Mail, die die Spam-Filterprüfung nicht besteht, wird mit den für Spam-Mails definierten Aktionen weiter bearbeitet. Wenn eine E-Mail alle Spam-Filter passiert und nicht als Spam identifiziert wird, erfolgt die nächste Stufe der Prüfung.

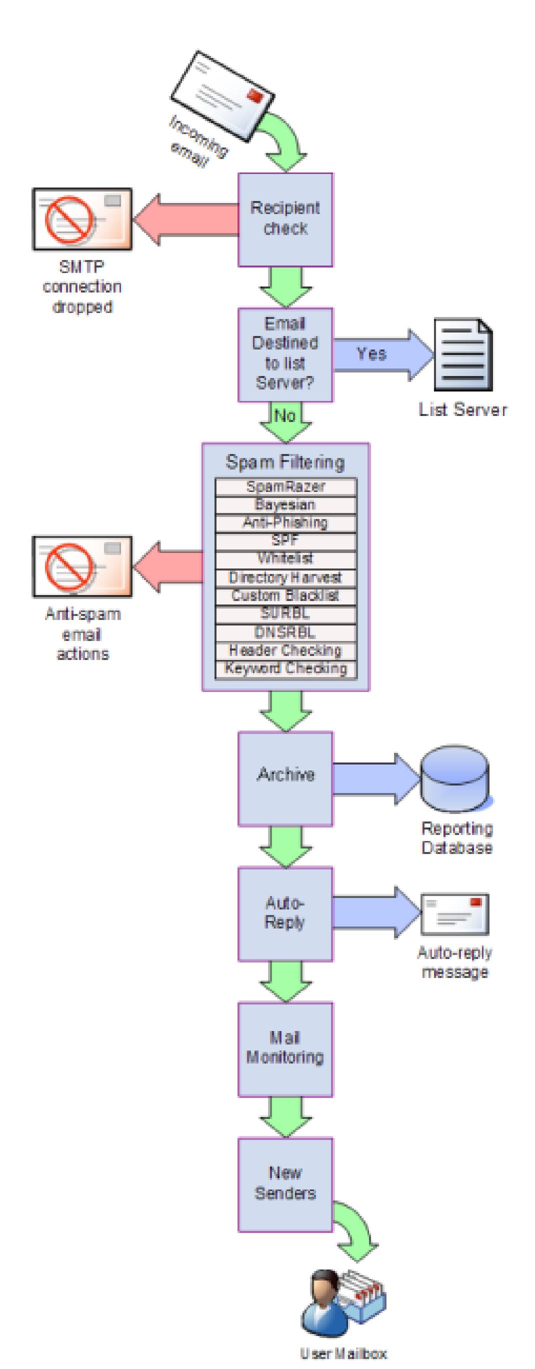
4. Bei entsprechender Konfiguration wird die E-Mail in der Berichtdatenbank archiviert. Danach erfolgt der Weitertransport der E-Mail zur nächsten Stufe.

5. Bei entsprechender Konfiguration werden automatische Antworten an den Absender gesendet. Die E-Mail wird in der nächsten Stufe weiterverarbeitet.

6. Bei entsprechender Konfiguration wird die E-Mail-Überwachung ausgeführt und es werden die entsprechenden Maßnahmen ergriffen. Die E-Mail wird in der nächsten Stufe weiterverarbeitet.

7. Der Filter "Neue Absender" wird ausgeführt. Die E-Mail wird in der nächsten Stufe weiterverarbeitet.

8. Die E-Mail wird in das Benutzerpostfach gesendet.



7.1.1 Domänen eingehender E-Mails

Ein sehr wichtiges Konzept bei GFI MailEssentials sind die Domänen eingehender E-Mails. Aufgrund seiner Konfiguration erkennt GFI MailEssentials automatisch die Domänen, bei denen Sie E-Mails empfangen. Auf diese Weise können Sie zwischen eingehenden und ausgehenden E-Mails unterscheiden und Ihr Netzwerk gegen Spam schützen. Domänen eingehender E-Mails können nach der Installation über die Konfigurationskonsole von GFI MailEssentials konfiguriert werden. Weitere Informationen finden Sie in der Anleitung "Administration und Konfiguration" von GFI MailEssentials.

7.2 Filtern ausgehender E-Mails

Das Filtern ausgehender E-Mails ist ein Vorgang, bei dem von den Benutzern versendete E-Mails im Unternehmen verarbeitet und dann erst abgesendet werden.

1. Der Benutzer erstellt und versendet E-Mails.

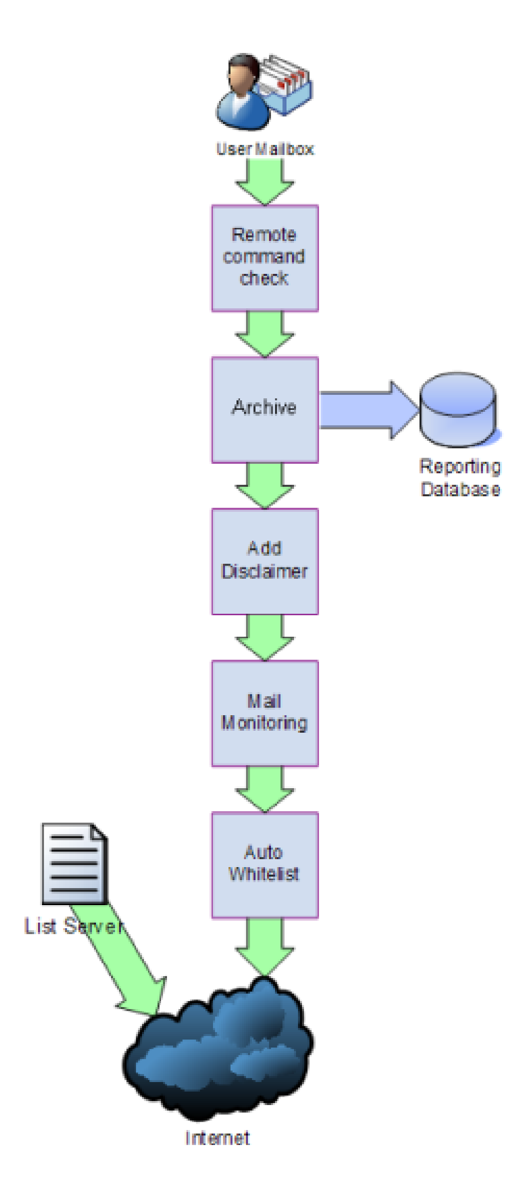
2. Die Funktion für Remote-Befehle sucht nach Remote-Befehlen in E-Mails und führt diese aus. Wenn keine gefunden werden, wird die E-Mail in der nächsten Stufe weiterverarbeitet.

3. Als Nächstes wird bei der E-Mail geprüft, ob sie archiviert werden soll. Wenn die Archivfunktion aktiviert ist, wird die E-Mail in der Berichtdatenbank gespeichert. In allen anderen Fällen wird die E-Mail in der nächsten Stufe weiterverarbeitet.

4. Bei entsprechender Konfiguration wird ein entsprechender Haftungsausschluss in der E-Mail ergänzt. Danach wird die E-Mail in der nächsten Stufe weiterverarbeitet.

5. Es wird für die E-Mail überprüft, ob eine E-Mail-Überwachung eingerichtet ist, und es werden entsprechend den gegebenenfalls konfigurierten Regeln Aktionen ausgeführt. Die E-Mail wird in der nächsten Stufe weiterverarbeitet.

6. Bei entsprechender Aktivierung ergänzt die automatische Prüfung der Whitelist die E-Mail-Empfängeradresse in der Whiteliste. Damit können automatisch Antworten von solchen Empfängern an den Absender gesendet werden, ohne dass eine Überprüfung erfolgt. Nach dieser Prüfung werden die E-Mails an die Empfänger versendet.



Die Sequenz für ausgehende E-Mails gilt für alle ausgehenden E-Mails mit Ausnahme der Prozesse für ausgehende E-Mails, die über den Listen-Server gestartet werden. Mit dieser Funktion können Sie Verteilerlisten anlegen und von GFI MailEssentials umleiten (Newsletter - und Diskussionslisten). In diesem Fall werden E-Mails auf Spam gescannt und automatisch an die Empfänger versendet.

8 Anhang 2 - Einsatz des Bayes-Filters

Der Bayes-Filter ist ein Anti-Spam-Verfahren in GFI MailEssentials. Er arbeitet mit einem adaptiven Verfahren auf der Grundlage künstlicher Intelligenz und erkennt die meisten heute üblichen Spam-Verfahren.

Dieses Kapitel erläutert, wie der Bayes-Filter funktioniert, wie er konfiguriert ist und wie er trainiert werden kann.

HINWEIS: Der Bayes-Filter ist standardmäßig deaktiviert. Bevor Sie den Bayes-Filter aktivieren, sollten Sie ihn trainieren.

WICHTIGER HINWEIS: GFI MailEssentials muss mindestens eine Woche arbeiten, damit der Bayes-Filter optimal funktioniert. Dies ist deswegen erforderlich, weil der Bayes-Filter seine Höchsterkennungsrate nur dann erreicht, wenn er sich an Ihre E-Mail-Muster anpasst.

Wie funktioniert der Bayes-Filter?

Der Bayes-Filter geht davon aus, dass die meisten Ereignisse zusammenhängen und dass aus den früheren Häufigkeiten dieses Ereignisses die Wahrscheinlichkeit abgeleitet werden kann, mit der ein Ereignis in Zukunft eintritt.

HINWEIS: Weitere Informationen über die mathematischen Grundlagen des Bayes-Filters finden Sie unter den folgenden Links:

http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html

http://www.niedermayer.ca/papers/bayesian/bayes.html

Das gleiche Verfahren wird von GFI MailEssentials verwendet um Spam zu identifizieren und zu klassifizieren. Dabei geht man davon aus, dass ein bestimmtes Textstück in Spam-Mails häufig auftritt, nicht jedoch in den zulässigen E-Mails, und die betreffende E-Mail daher mit gewisser Wahrscheinlichkeit Spam ist.

Erstellen einer benutzerdefinierten Bayes-Wortdatenbank

Bevor ein Bayes-Filter verwendet wird, muss eine Datenbank mit Worten und Token, beispielsweise Dollarzeichen, IP-Adressen und Domänen usw. erstellt werden. Diese kann aus einer Stichprobe von Spam-Mails und zulässigen E-Mails erstellt werden (sogenanntem 'HAM').

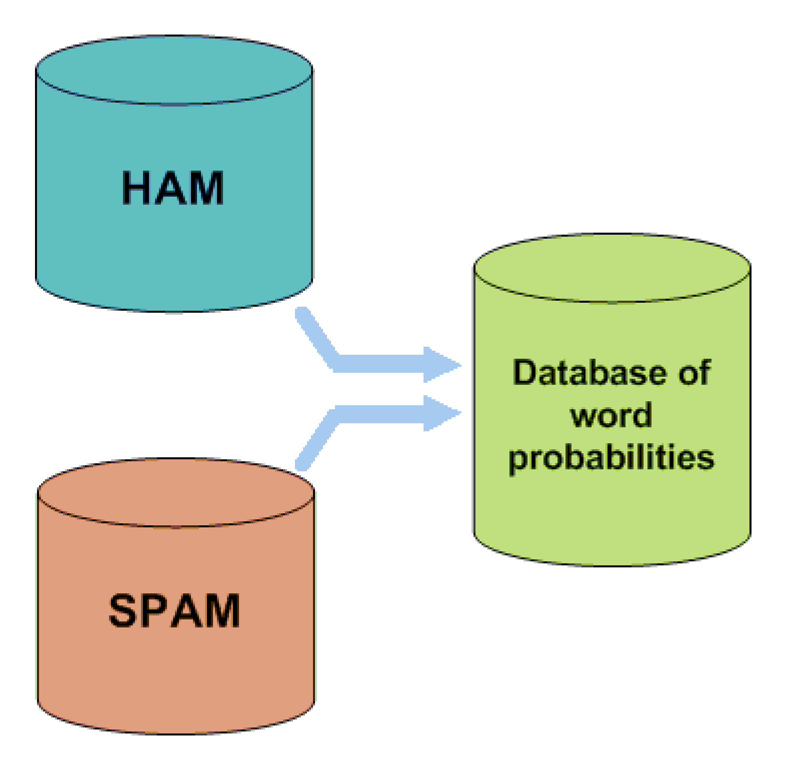


Abbildung 1 - Erstellen einer Wortdatenbank für den Filter

Anschließend wird jedem Wort oder Token ein Wahrscheinlichkeitswert zugeordnet; dieser Wert richtet sich danach, wie oft dieses Wort in SPAM, nicht aber in HAM vorkommt. Dazu werden die ausgehende E-Mails der Benutzer und bekannte Spam-Mails analysiert: Alle Wörter und Token, die in beiden E-Mail-Gruppen auftauchen, werden analysiert um die Wahrscheinlichkeit zu ermitteln, dass ein bestimmtes Wort in einer Spam-Mail auftaucht.

Diese Wahrscheinlichkeit wird nach folgendem Beispiel berechnet:

Wenn das Wort 'Hypothek' - in 400 von 3000 Spam-Mails auftaucht und in 5 von 300 zulässigen E-Mails, liegt die Spam-Wahrscheinlichkeit bei 0,8889 (das heißt [400/3000] / [5/300 + 400/3000]).

Erstellen einer benutzerdefinierten Datenbank mit zulässigen E-Mails

Die Analyse zulässiger E-Mails erfolgt mit den Firmen E-Mails und wird somit für die betreffende Firma angepasst.

- **Beispiel:** Ein Finanzinstitut verwendet möglicherweise das Wort 'Hypothek' häufig und würde viele falsch-positive Treffer erhalten, wenn eine allgemeine Anti-Spam-Regel definiert ist. Der Bayes-Filter andererseits erkennt, wenn er während einer ersten Trainingsphase für Ihr Unternehmen angepasst wird, was gültige ausgehende E-Mails des Unternehmens sind (und dass das Wort Hypothek häufig in zulässigen E-Mails verwendet wird); somit hat er eine wesentlich bessere Spam-Erkennungsrate und eine weit niedrigere Zahl falsch-positiver Treffer.

Erstellen der Bayes-Spam-Datenbank

Neben zulässigen E-Mails (HAM) wertet der Bayes-Filter auch eine

Spam-Datendatei aus. Diese Spam-Datendatei muss eine große Zahl bekannter Spam-Mails enthalten. Außerdem muss sie laufend mit den neuesten Spam-Nachrichten von der Anti-Spam-Software aktualisiert werden. Auf diese Weise kennt der Bayes-Filter immer die neuesten Spam-Trends und erzielt eine höhere Spam-Erkennungsrate.

Wie funktioniert der Bayes-Filter?

Sobald die Datenbank für zulässige E-Mails und für Spam-Mails erstellt sind, kann die Wortwahrscheinlichkeit berechnet werden und der Filter ist einsatzbereit.

Sobald eine neue E-Mail eintrifft, wird sie in Wörter aufgeschlüsselt, und es werden die relevantesten Wörter (diejenigen, die zur Identifizierung, ob eine E-Mail Spam ist) identifiziert. Mit diesen Wörtern berechnet der Bayes-Filter die Wahrscheinlichkeit, dass eine neue Nachricht Spam ist. Ist die Wahrscheinlichkeit höher als ein bestimmter Schwellenwert, wird die Nachricht als Spam klassifiziert.

HINWEIS: Weitere Informationen zum Bayes-Filter und dessen Vorteilen finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID001813

9 Glossar

Active Directory	Ein Verfahren mit verschiedenen Netzwerkdiensten beispielsweise LDAP-ähnlichen Diensten
Anzeige	*Siehe* Active Directory
Automatische Antwort	Eine E-Mail-Antwort, die automatisch nach Eingang einer E-Mail versendet wird.
Bayes-Filter	Ein Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.
BITS	*Siehe*Intelligenter Hintergrund-Übertragungsdienst
Blacklist	Ein Verzeichnis der E-Mail-Benutzer beziehungsweise Domänen, von denen Benutzer keine E-Mails erhalten sollen.
Botnet	Eine Schadsoftware, die autonom und automatisch läuft und von einem Hacker/Cracker gesteuert wird.
Demilitarized Zone	Ein Bereich des Netzwerks, der nicht Teil des internen Netzwerkes ist, aber auch kein direkter Teil des Internets. Sie dient im Prinzip als Gateway zwischen internen Netzwerken und dem Internet.
DMZ	*Siehe* Demilitarized Zone
DNS	*Siehe* Domain Name System
DNS MX	*Siehe* Mail Exchange
Domain Name System	Eine Datenbank in TCP/IP-Netzwerken, die die Übersetzung von Host-Namen in IP-Nummern erlaubt und andere Domänen-Informationen enthält.
Echtzeitblockliste	Onlinedatenbanken mit Spam-IP-Adressen Eingehende E-Mails werden mit dieser Liste abgeglichen um zu erkennen, ob sie von Benutzern stammen, die auf einer Blacklist stehen.
E-Mail-Überwachungsregeln	Regeln, die die Replikation der E-Mails zwischen E-Mail-Adressen erlauben.
Falsch-positive Treffer	Ein falsches Ergebnis, das eine E-Mail als Spam-Mail identifiziert, obwohl sie es nicht ist.
Haftungsausschluss	Eine Erklärung, die den Umfang der Rechte und Pflichten von E-Mail-Empfängern begrenzt oder definiert.
Ham	Zulässige E-Mail
IIS	*Siehe* Internet-Informationsdienste
IMAP	*Siehe* Internet Message Access Protocol
Intelligenter Hintergrund-Übertragungsdienst	Eine Komponente des Windows-Betriebssystems, die die Übertragung von Dateien zwischen Systemen unter Nutzung der leeren Netzwerkbandbreite unterstützt.
Internet Message Access Protocol	Eines der beiden am häufigsten verwendeten Internetstandardprotokolle zum Laden von E-Mails, das andere ist POP3.

Internetinformationsdienste	Eine Reihe von Internetdiensten der Microsoft Corporation für Internetserver
LDAP	*Siehe* Lightweight Directory Access Protocol
Lightweight Directory Access-Protokoll	Ein Anwendungsprotokoll zur Abfrage und Bearbeitung von Verzeichnisdiensten unter TCP/IP
Listenserver	Eine spezielle Nutzungsart für E-Mail-Systeme, die die umfassende Verbreitung von E-Mails an mehrere E-Mail-Benutzer über Diskussionslisten oder Newsletter erlaubt.
Mail Exchange	Ein Eintrag der DNS für Namen anderer Einheiten, an die Mail gesendet werden soll.
MAPI	*Siehe* Messaging Application Programming Interface
MDAC	*Siehe* Microsoft Data Access Components.
Messaging Application Programming Interface	Eine Nachrichtenarchitektur und eine auf dem Komponenten-Objektmodell basierende Anwendungsprogrammierschnittstelle für Microsoft Windows.
Microsoft Data Access Components	Eine Windows-Technologie, mit der Entwickler eine homogene und konsistente Möglichkeit zur Entwicklung von Software erhalten, die auf fast jeden Datenspeicher zugreifen kann.
Microsoft Message Queuing Services	Eine Implementierung einer Warteschlange für Windows-Server-Betriebssysteme.
MIME	*Siehe* Multipurpose Internet Mail Extensions
MSMQ	*Siehe* Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	Ein Standard, der das Format von E-Mail so erweitert, dass nicht nur ASCII-Text unterstützt wird, sondern auch anderer Text, Anhänge, die kein Text sind, Nachrichtentexte mit mehreren Teilen und Header-Daten mit anderen als ASCII-Zeichensätzen.
NDR	*Siehe* Unzustellbarkeitsbericht.
Öffentlicher Order	Ein gemeinsamer Ordner, mit dem Microsoft Exchange-Benutzer Informationen austauschen können.
Perimeter Server/Gateway	Der Computer (Server) in einem Netzwerk, der direkt mit einem externen Netzwerk verbunden ist. In GFI MailEssentials bezieht sich der Begriff Perimeter Gateway auf die E-Mail-Server im Unternehmen, die E-Mails direkt von externen Domänen erhalten.
Phishing	Die Sammlung sensitiver persönlicher Daten mit Betrugsabsicht in der Regel mit Hilfe gefälschter Nachrichten.
POP2Exchange	Ein System, das E-Mail-Nachrichten von POP3-Mailboxen holt und an den E-Mail-Server weiterleitet.
POP3	Siehe Post Office Protocol ver.3
Post Office Protocol ver.3	Ein Protokoll für lokale E-Mail-Clients um E-Mails aus Postfächern über eine TCP/IP-Verbindung zu laden.
RBL	Siehe dazu Echtzeitblockliste.
Remote-Befehle	Anweisungen, die es erlauben, Aufgaben aus der Ferne auszuführen.
Secure Sockets Layer	Ein Protokoll, das die sichere und ganzheitliche Kommunikation zwischen Netzwerken gewährleistet.
Simple Mail Transfer-Protokoll	Ein Internetstandard für die E-Mail-Übertragung zwischen IP-Netzwerken.

SMTP	Siehe Simple Mail Transport Protocol.
Spam-Aktionen	Aktionen für eingegangene Spam-Mails, beispielsweise das Löschen der Spam-Mails oder Versand in einen Junk-Ordner.
SSL	Siehe Secure Sockets Layer.
Unzustellbarkeitsbericht	Eine automatische E-Mail-Nachricht, die den Absender informiert, dass eine E-Mail nicht zugestellt werden konnte.
WebDAV	Eine HTTP-Erweiterungsdatenbank, mit der Benutzer Dateien aus der Ferne interaktiv verwalten können. Zur Verwaltung von E-Mails in dem Postfach und dem öffentlichen Ordner in Microsoft Exchange.
Whitelist	Eine Liste der E-Mail-Adressen und Domänen, von denen laufend E-Mails eingehen.
Zombie	*Siehe* Botnet.

10 Index

P

R

S

U

V

W

Z